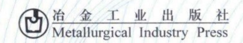


WULIANWANG
YINGYONG JISHU
XILIE JIAOCAI

现代无线传感网概论

无线龙 编著





现代
无线传感网概论



ISBN 978-7-5024-5696-2
9 787502 456962 >

定价40.00元
销售分类建议：计算机技术

★★★★ ★★★★

物联网应用技术系列教材

现代无线传感网概论

无线龙　编著

北　京
冶　金　工　业　出　版　社
2011

内容提要

本书共分4章，主要内容包括：无线传感网发展历程、现代无线传感网开发环境、现代无线传感网技术、现代无线传感网系统设计实例等。全书从无线传感网历史讲起，比较详细地描述了无线传感器网络涉及的关键技术和基本理论，结合相关实验和关键源代码，举例说明了具体设计传感器网络应用系统的方法，使理论与具体的实践相结合。

本书可作为高等学校或职业技术学院物联网和无线传感器网络专业概论课程的教学用书，也可供具有一定单片机和嵌入式基础的电子工程师和无线传感器网络从业人员参考。

图书在版编目(CIP)数据

现代无线传感网概论/无线龙编著. —北京：冶金工业出版社，2011.8

物联网应用技术系列教材

ISBN 978-7-5024-5696-2

Ⅰ.①现… Ⅱ.①无… Ⅲ.①无线电通信—传感器—高等学校—教材 Ⅳ.①TP212

中国版本图书馆CIP数据核字(2011)第159910号

出版人　曹胜利

地　　址　北京北河沿大街嵩祝院北巷39号，邮编100009

电　　话　(010)64027926　电子信箱　yjcbs@cnmip.com.cn

责任编辑　廖　丹　程志宏　美术编辑　李　新　版式设计　孙跃红

责任校对　石　静　责任印制　牛晓波

ISBN 978-7-5024-5696-2

北京兴华印刷厂印刷；冶金工业出版社发行；各地新华书店经销

2011年8月第1版，2011年8月第1次印刷

787mm×1092mm　1/16；18印张；431千字；274页

40.00元

冶金工业出版社发行部　电话:(010)64044283　传真:(010)64027893

冶金书店　地址:北京东四西大街46号(100010)　电话:(010)65289081(兼传真)

(本书如有印装质量问题，本社发行部负责退换)

《现代无线传感网概论》编委会

前　言

加快“感知中国”计划，加快物联网、传感网发展已经上升为国家战略。为了适应这个新形势，不少高校都在筹备建立物联网学院和物联网、传感网专业。最近教育部也要求高校逐步建立物联网、传感网专业，加快物联网、传感网相关技术普及和人才培养。

物联网、传感网是一项全新的技术，涉及微波、高频技术、嵌入式设计、低功耗无线技术、自组织无线网络技术、传感器技术、加密技术、智能技术等，因此目前还缺乏较全面介绍物联网技术的基础高校教材。本书作为高等教育概论性教材，从无线传感网历史讲起，比较详细地描述了无线传感器网络涉及的关键技术和基本理论，结合相关实验和关键源代码，举例说明了具体设计传感器网络应用系统的方法，使理论与具体的实践相结合。

注重基础知识和理论是本书的一大亮点，特别是第3章对MAC协议和结合AODV等算法对无线网状网络路由协议的分析和深入讨论，抓住了无线传感器网络技术核心，可使读者对无线传感器网络的技术基础和理论，有比较透彻的理解，具有一定理论深度。

本着厚基础、突出知识点的原则，本书适合作为高等院校和职业学院物联网和无线传感器网络专业概论课程的教学用书。通过全书的实际教学，可以让学生对物联网或无线传感器网的基础理论、核心算法和基础技术及关键技术，有一个全景式的了解和全方位接触，为进一步深入学习和研究打下基础。本书也适合于具有一定单片机和嵌入式基础的电子工程师自学和入门无线传感器网络。

物联网、传感网作为比互联网规模更为巨大的网络，必将进一步深入人类生活的方方面面，也就意味着除了物联网专业的学生学习和了解无线传感器网络技术外，应当有更多的其他专业的学生对无线传感器网络有概括性了解，例

如建筑类专业（选择各种楼宇监控、智慧家居等需要无线传感器网络部件和系统）、医学专业（选择各种嵌入人体的和医疗设备使用的无线传感器网络部件和系统等）、农业相关专业（选择温室监控、滴灌设备等使用的无线传感器网络部件和系统）、环境专业（选择各种水源、空气、环境检测使用无线传感器网络部件和系统）等。对于这些专业，采用本书作为物联网、无线传感器网络概论课程的教学用书也是非常合适的，可以让学生初步了解无线传感网技术基础和概貌。

为了加强理论和实际的结合，使学生在接受相关理论知识的同时，也获得相关实际技术和技能，本书配备有丰富的实验和相对应的教学实验箱和开放平台。在这些国产化实验箱和平台上，高校可以方便完成课堂演示和教学实验及实训。

加快普及物联网和无线传感网的知识和技术，加快感知中国的步伐，是我们和读者共同的心愿，我们衷心希望本书的出版能为物联网、传感网的教学和科研带来新动力，能为更多科研人员掌握物联网和无线传感器网络技术带来方便和惊喜。

最后感谢出版社编辑的指导和帮助，正是他们的努力，使这本书很快地出版，为物联网、无线传感器网络的百花园增加了嫣红一点。由于作者水平有限，书中难免存在不足，恳请广大读者批评指正。

作　者

2011 年 4 月

目　录

第1章 无线传感网发展历程

无线传感器网络（Wireless Sensor Networks，WSN，简称无线传感网或无线感知网）是当前在国际上备受关注的、涉及多学科高度交叉、知识高度集成的前沿热点研究领域。它综合了传感器技术、嵌入式计算技术、现代网络及无线通信技术、分布式信息处理技术等，能够通过各类集成化的微型传感器协作地实时监测、感知和采集各种环境或监测对象的信息，这些信息通过无线方式被发送，并以自组多跳网络方式传送到用户终端，从而实现物理世界、计算世界以及人类社会三元世界的连通。

无线传感网以最小的成本和最大的灵活性，连接任何有通信需求的终端设备，采集数据（见图1-1），发送指令。若把无线传感网各个包含传感器的执行单元（节点）设备视为“豆子”，将一把“豆子”（可能100粒，甚至上千粒）任意抛撒开，经过有限的“种植时间”，就可从某一粒“豆子”那里得到其他任何“豆子”的信息。作为无线自组双向通信网络，传感网络能以最大的灵活性自动完成不规则分布的各种传感器与控制节点的组网，同时具有一定的移动能力和动态调整能力。

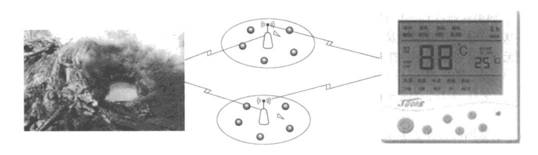


图1-1 数据采集

一个典型无线传感网的系统架构（见图1-2）包括分布式无线传感器节点（群）、接收发送器汇聚节点（网关）、数据中心（任务管理）等。大量传感器节点随机部署在监测区域内部或附近，能够通过自组织方式构成网络。传感器节点监测的数据沿着其他传感器节点逐跳地进行传输，在传输过程中监测数据可能被多个节点处理，经过多跳后路由到汇聚节点，最后通过互联网、卫星或其他方式传达到数据中心。传感器节点通常是一个微型嵌入式系统，它的处理能力、存储能力和通信能力相对较弱，通过携带能量有限的电池供电。

1.1 无线传感网在物联网的位置

2009年8月的太湖气候宜人，水面上微风吹拂，此时的湖边总少不了悠然的垂钓者和

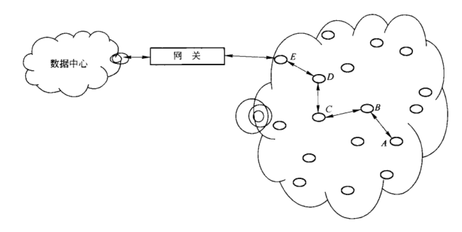


图 1-2 无线传感网

游客。2009 年 8 月，太湖附近的一个“建议”，使得一个概念在中国炙手可热，也使得一个新的产业逐渐浮出水面。

做出这个建议的人，是国务院总理温家宝，而“建议”的内容就是“尽快建立中国的传感信息中心，或者叫‘感知中国’中心”。

几乎在同一时刻，互联网搜索引擎中，“物联网”这个词汇的搜索量出现井喷，并从此在很长一段时间内维持在一个高位上。

如果你通过 Google 趋势搜索“物联网”这个词，你就会发现，对“物联网”的搜索量从无到有，搜索指数从 0 到 100 发生突变，而起点就是 2009 年 8 月 7 日温家宝考察中科院无锡高新微纳传感网工程技术研发中心，提出“感知中国”这个时间点开始的。

此后，8 月 24 日，中国移动总裁王建宙在台湾的一次演讲中公开提及“物联网”的概念；9 月 11 日，“传感器网络标准工作组成立大会暨‘感知中国’高峰论坛”在北京举行，这些都让这个新概念以一种近乎爆发的方式出现在人们眼前。

物联网的英文名字叫做“Internet of Things”，这个词，最早在 1999 年由 ITU（国际电信联盟）在一系列会议上被提及。而 2005 年，ITU 则把“Internet of Things”定为了其年度互联网报告的主题。

在这份仅摘要就长达 28 页的报告中，ITU 深入探讨了物联网的技术细节及其对全球商业和个人生活的影响，着重呈现了新兴技术、市场机会和政策问题等信息。报告由 ITU 战略与政策部撰写，而当时在 ITU 战略与政策部门任职的 Lara Srivastava 则参与了撰写过程。

目前，Lara 负责监控分析信息与通信技术、政策以及市场结构的趋势，尤其聚焦于移动及无线通信领域。在她看来，物联网并不是某种特定的技术，更像是一种愿景，一种对未来世界的描述，是多种技术的综合应用。而这种描述并非海市蜃楼，Lara 说物联网必然会带来很多新的商业模式，而这个过程已经开始了。

1.1.1 物联网

每一次大危机都会催生一些新技术，而新技术也是使经济特别是工业走出危机的巨大

推动力。2008 年以来席卷全球的金融危机也不例外，相关国家正在试图通过“物联网”走出经济的泥沼。

2008 年新一轮全球经济危机虽然起源于美国，但形成原因却非常复杂。由于金融在现代经济中地位突出，因此，当前全球在金融与经济领域出现的双重危机，较之过去历次经济危机而言，其影响深度及克服难度也更加复杂。

“注资救市”是各国政府应对此轮危机所采取的共同举措。鉴于此轮危机主要表现为金融领域和经济领域的双重危机，对于金融领域而言，适当的注资有利于避免由于资金链断裂而出现的多米诺骨牌效应；对于实体经济而言，过度的注资会使通胀的幽灵再次出现。

从人类历史长河来看，经济危机是经济发展过程中必然出现的产物，而人类应对经济危机的方式主要有两种，一为战争，即通过战争进行生产要素和消费要素的再分配，最终达到经济的均衡发展；二为新技术革命，即通过新一轮技术革命发展一批新兴产业，由新兴产业带动新的生产和消费需求，从而激发整个社会需求活力，使经济摆脱危机，进入新一轮由新技术革命推动的产业发展周期。

历史经验提示我们，与残酷的战争相比，新技术产业革命是解决经济危机的最佳手段，同时，任何一个大国的崛起或中兴都是建立在掌握世界当时最前沿科学技术基础上而实现的。就当今人类最前沿科学技术而言，无非是新动力能源（低碳经济）、基因工程、物联网等。由于基因工程尚有诸多难题没有答案，可以预计，此轮危机之后，率先走出危机并再度崛起的大国一定是掌握新动力能源（低碳经济）、物联网等革命核心技术的那个国家。

“物联网”概念问世，打破了之前的传统思维。过去的思路一直是将物理基础设施和 IT 基础设施分开：一方面是机场、公路、建筑物，而另一方面是数据中心、个人电脑、宽带等。而在“物联网”时代，钢筋混凝土、电缆将与芯片、宽带整合为统一的基础设施，在此意义上，基础设施更像是一块新的地球工地，世界的运转就在它上面进行，其中包括经济管理、生产运行、社会管理乃至个人生活。

物联网是把所有物品通过射频识别、感应器、定位系统、扫描器、视频跟踪等信息传感设备与网络连接起来，进行信息交换和通讯，实现智能化识别、定位、跟踪、监控和管理，如图 1-3 所示。

（1）对物体属性进行标识，属性包括静态和动态的属性，静态属性可以直接存储在标签中，动态属性需要先由传感器实时探测；

（2）需要识别设备完成对物体属性的读取，并将信息转换为适合网络传输的数据格式；

（3）将物体信息通过网络传输到信息处理中心（处理中心可能是分布式的，如家里电脑或者手机，也可能是集中式的，如中国移动 IDC），由处理中心完成物体通信相关计算。

物联网是在计算机互联网的基础上，利用 RFID、无线数据通信、传感等技术，构造一个覆盖世界上万事万物的“Internet of Things”。在这个网络中，物品（商品）能够彼此进行“交流”，而无需人的干预。其实质是利用射频自动识别（RFID）技术，通过计算机互联网实现物品（商品）的自动识别和信息的互联与共享。

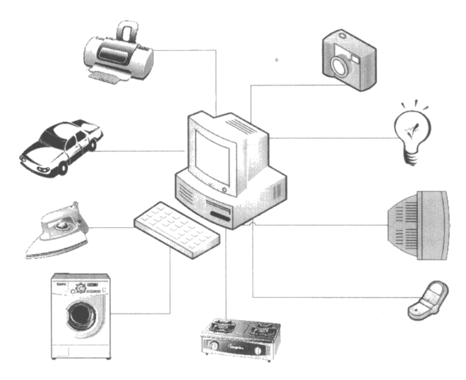


图 1-3 图解物联网

而 RFID，正是能够让物品“开口说话”的一种技术。在“物联网”的构想中，RFID 标签中存储着规范而具有互用性的信息，通过无线数据通信网络把它们自动采集到中央信息系统，实现物品（商品）的识别，进而通过开放性的计算机网络实现信息交换和共享，实现对物品的“透明”管理。

从信息流控制的角度，物联网由感知层、传送层和信息应用层等三层组成，即通过传感器等方式获取物理世界的各种信息，结合互联网、移动通信网等网络进行信息的传送与交互，采用智能计算技术对信息进行分析处理，从而提升对物质世界的感知能力，实现智能化的决策和控制。

物联网在组成上主要分为两个层面，一个是以传感和控制为主的硬件部分，主要由无线射频识别 RFID、传感、数据传输等技术构成，另一个方面主要的是以软件为主的数据处理技术，其中包括搜索引擎技术、数据挖掘、人工智能处理、实现人机交流的标准化机器语言等。

1.1.2 物联网体系

物联网是通过射频识别、感知器、定位系统、扫描器、传感器、图像感知器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络。

按照网络内数据的流向及处理方式将物联网分为三个层次（如图 1-4 所示）：一是感

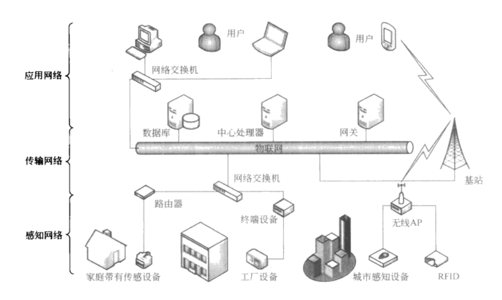


图 1-4 物联网架构

知网络层，即以二维码、RFID、传感器为主，实现对物、人或环境状态识别、感知；二是传输网络层，即通过现有的互联网、广电网、通信网或者下一代互联网，实现数据的传输、计算和存储；三是应用网络层，即输入输出控制终端，包括电脑、手机、笔记本等终端。

RFID 确实是实现物联网的关键性技术之一，它带来了实时捕获个体物品信息的可能性。其实 RFID 只是自动识别技术家族的一部分，这整个家族都是促进物联网的关键性技术，但是并不仅仅只有它们而已。

除了自动识别技术之外，另外一项很重要的技术是传感器，因为需要有一项技术把物品与互联网相连接。如果房间里有一个物品，其中是有 RFID 的，那么它所起的作用是告诉我们有这样一个东西是在那里的，但是更具体的信息我们并不知道，比如说，我们可以知道房间里有一把剪刀、一包牛奶，但是我们并不知道那包牛奶是否已经过期了，或者它是否被污染了，在这些方面就是传感器起作用的地方。传感器不仅仅能够告诉我们物品的存在，还能够告诉我们物品所处的环境、它所包含的物质等。

作为物联网的物物互联子网络，在感知层的（无线）传感网在很早以前就开始了相关研究。早在 1999 年，中国科学院就启动了传感网研究，由其提出的传感网络体系架构、标准体系、演进路线、协同架构等代表传感网络发展方向的顶层设计已被 ISO/IEC 国际标准认可。

传感网已经成为政府推进物联网发展的首要着力点，在政府高度关注和明确支持以及产业技术发展、需求推动等协同作用下，我国传感网市场将在未来一段时间内以超过 200% 的年均复合增长率增长，并于 2015 年达到 200 亿元人民币规模。

对于传感网，射频通信和感知设备是核心技术，也是利润最大产业。射频通信由于我国起步比较晚，因此在射频通信（无线芯片）方面比较薄弱，主要还是被国外所垄断，例

如TI和飞思卡尔等公司。

国内目前在无线传感器网络软件方面也取得了相应的突破，在基于国外的操作系统之上，开发了自己的中间件软件。如南京邮电大学无线传感器网络研究中心开发的基于移动代理的无线传感器网络中间件平台；无线龙科技C51RF-WSN无线传感器网络开发平台，提供了功能齐全的硬件开发平台，对外提供便捷的接口，使用户无需了解底层细节，极大地降低了无线传感器网络应用开发的难度。

国内研究机构在理论研究方面，如对无线传感器网络网络协议、算法、体系结构等方面，提出了许多具有创新性的想法与理论。在这方面，国内的南京邮电大学、哈尔滨工业大学、清华大学、上海交通大学、北京邮电大学等都取得了一些相关的理论研究成果。

目前国内比较成功的无线传感器网络软件产品包括：南京邮电大学的无线传感器网络中间件软件、南京邮电大学的无线传感器网络集成开发平台、无线龙科技C51RF-WSN无线传感器网络开发平台及中间件、中国科学院无线传感器网络分析与管理平台。

目前，我国传感网标准体系已初步建立框架，向国际标准化组织提交的多项标准提案被采纳，传感网标准化工作已经取得积极进展。经国家标准化管理委员会批准，全国信息技术标准化技术委员会组建了传感器网络标准工作组。标准工作组聚集了中国科学院、中国移动通信集团公司等国内传感网主要的技术研究和应用单位，积极开展传感网标准制定工作，深度参与国际标准化活动，旨在通过标准化为产业发展奠定坚实技术基础。

我国对传感网发展高度重视，《国家中长期科学与技术发展规划（2006—2020年）》和“新一代宽带移动无线通信网”重大专项中均将传感网列入重点研究领域。国内相关科研机构、企事业单位积极进行相关技术的研究，经过长期艰苦努力，攻克了大量关键技术，取得了国际标准制定的重要话语权，传感网发展具备了一定产业基础，在电力、交通、安防等相关领域的应用也初见成效。

1.2 无线传感网简史

信息的生成、获取、存储、传输、处理及其应用是现代信息科学的六大组成部分，其中信息获取是信息技术产业链上重要的环节之一，没有它就没有信息的传输、处理和应用，信息化也就成了无水之源、无本之木。

随着现代微电子技术、微机电系统（Micro Electrp Mechanism System，MEMS）、片上系统SoC（System on Chip）、纳米材料、无线通信技术、信号处理技术、计算机网络技术等的进步以及互联网的迅猛发展，传统传感器信息获取技术从独立的单一化模式向集成化、微型化，进而向智能化、网络化方向发展，成为信息获取最重要和最基本的技术之一。现代传感器如图1-5所示。

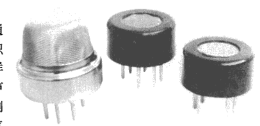


图1-5 现代传感器

传感网是集传感器、数据处理单元和通信模块的微小节点随机分布，并通过自组织方式构成的网络，借助节点中内置形式多样传感器测量所在周边环境中热、红外、声呐、雷达、射频和地震波等信号，从而探测包括温度、湿度、噪声、光强度、压力、气体成分及浓度、土壤成分、移动物体大小、

速度和方向等众多感兴趣的物质现象。在通信方式上，可以采用有线、无线、红外、超声波和光等任意一种或多种方式。

因此传感器网络可以根据通信方式分类为有线传感器网络、无线传感网、红外传感器网络、超声波传感器网络等。

一般认为采用无线通信技术的传感器网络称作无线传感网（Wireless Sensor Networks，WSN）。

无线传感网是从传感器网络开始的，传感器网络经历了如图1-6所示发展历程。

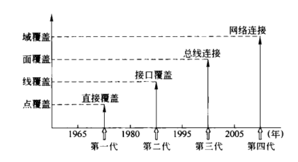


图1-6 传感器网络历史

第一代传感器网络出现在20世纪70年代，使用具有简单信息信号获取能力的传统传感器，采用点对点传输、连接传感控制器构成传感器网络。

第二代传感器网络，具有获取多种信息信号的综合能力，采用串/并接口（如RS-232、RS-485）与传感控制器相连，构成有综合多种信息的传感器网络。

第三代传感器网络出现在20世纪90年代后期和21世纪初，用具有智能获取多种信息信号的传感器，采用现场总线连接传感控制器，构成局域网络，成为智能化传感器网络。

第四代传感器网络正在研究开发，目前成形并大量投入使用的产品还没有出现，用大量的具有多功能多信息信号获取能力的传感器，采用自组织无线接入网络，与传感器网络控制器连接，构成无线传感网。

无线传感网是新兴的下一代传感器网络。最早的代表性论述出现在1999年，题为“传感器走向无线时代”。随后在美国的移动计算和网络国际会议提出，无线传感网是下一个世纪面临的发展机遇。2003年，美国《技术评论》杂志论述未来新兴十大技术时，无线传感网被列为第一项未来新兴技术。同年美国《商业周刊》未来技术专版，论述四大新技术时，无线传感网也列入其中。美国《今日防务》杂志更认为无线传感网的应用和发展，将引起一场划时代的军事技术革命和未来战争的变革。2004年（IEEE Spectrum）杂志发表一期专集：传感器的国度，论述无线传感网的发展和可能的广泛应用。可以预计，无线传感网的发展和广泛应用，将对人们的社会生活和产业变革带来极大的影响和产生巨大的推动。

总体来说，无线传感网思想起源于20世纪70年代；1978年DARPA在卡耐基-梅隆大学成立了分布式传感器网络工作组；1980年DARPA的分布式传感器网络项目（DSN）开启了传感器网络研究的先河；20世纪80～90年代，研究主要在军事领域，成为网络中心战的关键技术，拉开了无线传感网研究的序幕；20世纪90年代中后期，无线传感网引起

了学术界、军界和工业界的广泛关注，发展了现代意义的无线传感网技术。

1.2.1 国外研究现状

美国军方最先开始无线传感网技术的研究，开展了包括有 CEC、REMBASS、TRSS、Sensor IT、WINS、Smart Dust、Sea Web、μAMPS、NEST 等研究项目。美国国防部远景计划研究局已投资几千万美元，帮助大学进行无线传感网技术的研发。

美国国家自然基金委员会（NSF）也开设了大量与其相关的项目，NSF 于 2003 年制定 WSN 研究计划，每年拨款 3400 万美元支持相关研究项目，并在加州大学洛杉矶分校成立了传感器网络研究中心。2005 年对网络技术和系统的研究计划中，主要研究下一代高可靠、安全的可扩展的网络，可编程的无线网络及传感器系统的网络特性，资助金额达到 4000 万美元。此外，美国交通部、美国能源部、美国国家航空航天局也相继启动了相关的研究项目。

美国所有著名院校几乎都有研究小组在从事 WSN 相关技术的研究，加拿大、英国、德国、芬兰、日本和意大利等国家的研究机构也加入了 WSN 的研究。加州大学洛杉矶分校、加州大学伯克利分校、麻省理工学院、康奈尔大学、哈佛大学、卡耐基-梅隆大学等在 WSN 研究领域成绩较为突出。国际相关学术会议对 WSN 的研讨增多，检索论文数目逐年以较大幅度增加。美国的 Crossbow、Dust Network、Ember、Chips、Intel、Freescale 等公司也开展了 WSN 的研究工作。

加拿大、英国、德国、芬兰、日本和意大利等国家的研究机构也加入了 WSN 计划。欧盟第 6 个框架计划将“信息社会技术”作为优先发展领域之一。其中多处涉及对 WSN 的研究。启动了 EYES 等研究计划。日本总务省在 2004 年 3 月成立了“泛在传感器网络”调查研究会。韩国信息通信部制订了信息技术“839”战略，其中“3”是指 IT 产业的三大基础设施，即宽带融合网络、泛在传感器网络、下一代互联网协议。企业界中，欧盟的 Philips、Siemens、Ericsson、ZMD、France Telecom、Chipcon 等公司；日本的 NEC、OKI、SKYLEYNETWORKS、世康、欧姆龙等公司都开展了 WSN 的研究。

1.2.2 国内研究现状

无线传感网技术的研究首次正式启动出现于 1999 年中国科学院《知识创新工程点领域方向研究》的“信息与自动化领域研究报告”中，是该领域的五大重点项目之一。2001 年中国科学院依托上海微系统所成立微系统研究与发展中心，旨在引领中科院 WSN 的相关工作。

国家自然科学基金已经审批了 WSN 相关的一个重点课题和多项课题。2004 年将一项无线传感网项目（面上传感器网络的分布自治系统关键技术及协调控制理论）列为重点研究项目。2005 年将网络传感器中的基础理论和关键技术列入计划。2006 年将水下移动传感器网络的关键技术列为重点研究项目。国家发改委下一代互联网（CNGI）示范工程中，也部署了 WSN 的相关课题。

在一份我国未来 20 年预见技术的调查报告中，信息领域 157 项技术课题中有 7 项与传感器网络直接相关。2006 年初发布的《国家中长期科学与技术发展规划纲要》为信息技术定义了三个前沿方向，其中两个与无线传感网研究直接相关，即智能感知技术和自组

织网络技术。我国2010年远景规划和“十五”计划中将WSN列为重点发展的产业之一。

随着无线传感网技术ZigBee无线网络发展，国内许多企业及高校正在加强无线传感网研究及开发。

ZigBee是一种新兴无线网络通信规范，主要用于近距离无线连接。ZigBee的基础是IEEE无线个域网工作组所制定的IEEE802.15.4技术标准口。802.15.4标准旨在为低能耗简单设备提供有效覆盖范围在100m左右的低速连接，可广泛用于交互玩具、库存跟踪监测等消费与商业应用领域。

ZigBee当然不仅只是802.15.4的名字。IEEE802.15.4仅处理低级MAC层和物理层协议，ZigBee联盟对其网络层协议和API进行了标准化，还开发了安全层，以保证这种便携设备不会意外泄漏其标识，而且这种利用网络的远距离传输不会被其他节点获得。此外ZigBee还具有低传输速率、低功耗、协议简单、时延短、安全可靠、网络容量大、优良的网络拓扑能力等优点。

ZigBee这些优点极好地支持了无线传感网：它能够在众多微小的传感器节点之间相互协调实现通信，这些节点只需要很低的功耗，以多跳接力的方式在节点间传送数据，因而通信效率非常高。目前ZigBee联盟正在进行协议标准的应用推广工作，该标准的成功制定对于无线传感网的推广使用将有着深远、重要的意义。

1.3 无线传感网体系和结构

在传感器网络中，节点可以通过飞机布撒或人工闲置等方式，大量部署在被感知对象内部或者附近。这些节点通过自组织方式构成无线网络，以协作的方式实时感知、采集和处理网络覆盖区域中的信息，并通过多跳网络将数据经由Sink节点（或称为聚合节点或网关）链路将整个区域内的信息传送到远程控制管理中心。反之远程管理中心也可以对网络节点进行实时控制和操纵。

无线传感网结构如图1-7所示，整个网络主要包括以下几部分：

（1）管理中心（数据中心）。它负责从网络中获取所需要的信息，同时也可以对网络

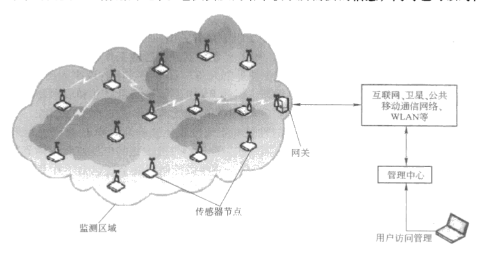


图1-7 无线传感网结构

做出各种各样的指示、应用支撑技术操作等。

(2) 传输介质（有线网络如互联网或通讯卫星）。它是管理中心与传感网络之间的桥梁和纽带。

(3) Sink节点（或称为聚合节点或网关）。在传输前聚集收到的数据以便节省传输能量，聚合通过每个节点类型和不同应用特有的过滤器实现。它拥有足够的能量，可以将从传感器网络中的能量有限的节点上传来的信息转发到传输介质上。

(4) 传感器节点。负责数据采集及数据传输。

(5) 传感网络。这是传感器网络的核心。在感知区域中，大量的节点自组成网，监测、感知信息向Sink节点发送，或接收来自Sink节点的操作命令，改变自身的工作状态。

1.3.1 传感器节点

在不同应用中，传感器节点的组成不尽相同，但一般都由数据采集、数据处理、数据传输和电源这4部分组成（见图1-8）。根据具体应用需求，还可能会有定位系统以确定传感节点的位置，有移动单元使得传感器可以在待监测地域中移动，或具有供电装置以从环境中获得必要的能源。此外，还必须有一些应用相关部分，例如，某些传感器节点有可能在深海或者海底，也有可能出现在化学污染或生物污染的地方，这就需要在传感器节点的设计上采用一些特殊的防护措施。

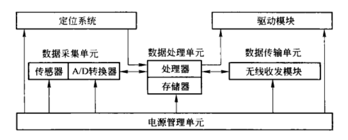


图1-8 传感器节点结构

无线传感网节点典型配置包括几个主要组成部分：RF收发器（模拟器件，工作频率为300MHz～2.4GHz的ISM高频频段）、MCU（数字器件，通常工作在kHz～MHz的低频频段）和传感器。RF收发器通常带有各种外部元件，如电感、电容或声表面波滤波器。由于这些外部元件体积庞大而且成本较高，因此RF电路很难满足尺寸和成本要求。随着CMOS工艺迅速进步，目前市面上出现了一些小型的低成本高集成度RF收发器。

与此同时，现成的工业微控制器的性能和集成度也迅速提高。MCU集成了越来越多的外围电路，成本却没有增加太多。例如一些微控制器带有内建的电压监测、调节器、温度传感器等，而此前这些都是MCU外部元件。一些微控制器甚至还包括了片上低功耗实时时钟和硬件加密模块，减小了数字电路的尺寸和成本。

这些“组合”芯片的出现令人鼓舞，目前多家公司正在推出集成了RF收发器和MCU的单芯片产品。由于RF和数字电路之间存在串扰和噪音问题，以前很难实现两者集成，随着CMOS RF技术不断改进，现在可设计出RF-数字集成芯片，进一步减小了产品尺寸和降低了产品的生产成本。

微电机系统、低功耗无线电路和数字电路设计的飞速发展在很大程度上加快了这种无线传感网应用。

无线传感网的一个重要优势是摆脱了传统网络的连线限制和成本问题。但是如果没有合适的无线电源，这一优势就无法体现出来，因此电源效率是设计考虑的关键因素，因为如果必须时常更换电池（例如每周或每月），那么相关的劳动力成本便会远远超过它相对有线网络节省的成本。因此电池必须具有较长的寿命（通常几个月到10年）。此外由于传感器网络的理念是“随时随地无线”，减小节点尺寸也是必须考虑的设计要素，对传感器节点来说，很多时候即使采用AA电池也会超出体积要求，因此只能选择纽扣式电池供电。

传感器节点能量的供应是采用电池，节点能量有限，考虑尽可能地延长整个传感器网络的生命周期，在设计传感器节点时，保证能量供应的持续性是一个重要的设计原则。传感器节点能量消耗的模块主要是包括传感器模块、信息处理模块和无线通讯模块，而绝大部分的能量消耗是集中在无线通讯模块上，约占整个传感器节点能量消耗的80%。因此，目前提出的传感器节点通讯路由协议主要是围绕着减少能量消耗，延长网络生命周期而进行设计的。

在无线传感网中，节点在不同的状态具有不同的能量消耗，传感器节点共有6种工作状态。

（1）睡眠状态：传感器模块关闭，通信模块关闭，能量消耗最低；

（2）感知状态：传感器模块开启，通信模块关闭，节点感知事件发生；

（3）侦听状态：传感器模块开启，通信模块空闲；

（4）接收状态：传感器模块开启，通信模块接收；

（5）发送状态：传感器模块开启，通信模块发送；

（6）长期睡眠状态：表示该节点能量已低于阀值，不响应任何事件。

目前无线传感网的功耗可降低到毫安级甚至微安级以下，因此传感器节点可使用一颗3V直流纽扣式电池来供电，根据不同的采样率，其工作时间可以达五年或以上。采用纽扣式电池的此类传感器节点外形小巧，便于携带且易于设计到小型设备中。这些低功耗、低数据率的应用包括工厂中各种精密数字辅助测量仪器，如水表和煤气抄表、供应链出货量监测和个人标记佩戴报告等。这些应用有三个共同要求：外形小、电池寿命长以及具有鲁棒特性，满足这些要求的前提条件是选择适当的网络结构。

1.3.2 传感器网络

无线传感网的传感器网络相对于传统网络，其最明显的特色可以用六个字来概括，即“自组织，自愈合”。自组织是指在无线传感网中不像传统网络需要人为指定拓扑结构，其各个节点在部署之后可以自动探测邻居节点并形成网状的最终汇聚到网关节点的多跳路由，整个过程不需人为干预。同时整个网络具有动态鲁棒性，在任何节点损坏，或加入新节点时，网络都可以自动调节路由随时适应物理网络的变化。这就是所谓的自愈合特性。

这些特点使得无线传感网能够适应复杂多变的环境，去监测人力难以到达的恶劣环境地区。汶川地震发生之后所有通信设施中断，在后期只能依靠人力对余震、山体滑坡、堰塞湖等进行检测，效率低下，且缺乏量化数据进行科学分析预测。如果能够在灾区部署无

线传感网就能有效地解决这一问题。

无线传感网节点体积大多小巧，电池供电可以保证数月工作时间，不需现场拉线供电，非常方便在应急情况下进行灵活部署监测并预测地质灾害的发生情况。

因汶川地震而形成的唐家山堰塞湖，在湖区不同位置安置配备液位传感器的无线节点实时监测水位变化状况，再汇总至监控中心后，就可以结合地理位置信息和历史数据，形成三维数据，观察水位变化趋势，推导对坝体压力以及在关键点水深超过危险门限值时自动产生报警信息。其部署效率和能够为决策者提供的信息量都远远超过单纯的人力监测。

当然这只是一种设想。我们希望的是能够从这次灾害中归纳提炼出一些无线传感网方案，在以后遇到类似灾害时可以更加有效率地去救灾，能够减轻解放军战士的工作量和为救灾专家们提供更多更简单的手段，就像地震中得到广泛应用的生命探测仪一样。

网络体系结构是网络的协议分层以及网络协议的集合，是对网络及其部件所应完成功能的定义和描述。对无线传感网来说，其网络体系结构不同于传统的计算机网络和通信网络。网络体系结构由分层的网络通信协议、传感器网络管理以及应用支撑技术三部分组成。

分层的网络通信协议结构类似于TCP/IP协议体系结构；传感器网络管理技术主要是对传感器节点自身的管理以及用户对传感器网络的管理；在分层协议和网络管理技术的基础上，支持了传感器网络的应用支撑技术。

传感器网络体系结构具有二维结构，即横向的通信协议层和纵向的传感器网络管理面。通信协议层可以划分为物理层、链路层、网络层、传输层、应用层，而网络管理面则可以划分为能耗管理面、移动性管理面以及任务管理面。

管理面的存在主要是用于协调不同层次的功能以求在能耗管理、移动性管理和任务管理方面获得综合考虑的最优设计。

1.4 无线传感网应用领域

无线传感网是由部署在监测区域内部或附近的大量廉价的具有通信、感测及计算能力的微型传感器节点通过自组织构成的“智能”测控网络。无线传感网在军事、农业、环境监测、医疗卫生、工业、智能交通、建筑物监测、空间探索等领域有着广阔的应用前景和巨大的应用价值，被认为是未来改变世界的十大技术之一、全球未来四大高技术产业之一。

传感器网络的应用与具体的应用环境密切相关，因此针对不同的应用领域，存在性能不同的无线传感网系统。

1.4.1 军事领域

无线传感网具有可快速部署、可自组织、隐蔽性强和高容错性的特点，因此非常适合在军事上应用。利用无线传感网能够实现对敌军兵力和装备的监控、战场的实时监视、目标的定位、战场评估、核攻击和生物化学攻击的监测和搜索等功能。目前国际许多机构的课题都是以战场需求为背景展开的。例如，美军开展的如C4KISR计划、Smart Sensor Web、灵巧传感器网络通信、无人值守地面传感器群、传感器组网系统、网状传感器系统

CEC 等。

在军事领域应用方面，该项技术的远景目标是：利用飞机或火炮等发射装置，将大量廉价传感器节点按照一定的密度布放在待测区域内，对周边的各种参数，如温度、湿度、声音、磁场、红外线等各种信息进行采集，然后由传感器自身构建的网络，通过网关、互联网、卫星等信道，传回信息中心。

该技术可用于敌我军情监控。在友军人员、装备及军火上加装传感器节点以供识别，随时掌控自己情况。通过在敌方阵地部署各种传感器，做到知己知彼，先发制人。另外，该项技术可用于智慧型武器的引导器，与雷达、卫星等相互配合，利用自身接近环境的特点，可避免盲区，使武器的使用效果大幅度提升。

美国军方研究的用于军事侦察的 NSOF（Networked Sensors for the Objective Force）系统是美国军方目前研究的未来战斗系统的一部分，能够收集侦查区域的情报信息并将此信息及时地传送给战术互联网。系统由大约 100 个静态传感器和用于接入战术互联网的指挥控制节点 C2（command and control）构成，系统架构如图 1-9 所示。



图 1-9　NSOF 系统

1—狙击手的位置；2—节点位置

2005 年美国军方构建了枪声定位系统，节点部署于目标建筑物周围，系统能够有效地自组织构成监测网络，监测突发事件（如枪声、爆炸等）的发生，为救护、反恐提供了有力的帮助。

美国科学应用国际公司采用无线传感网构建了一个电子防御系统，为美国军方提供军事防御和情报信息。系统采用多个微型磁力计传感器节点来探测监测区域中是否有人携带枪支、是否有车辆行驶，同时，系统利用声音传感器节点监测车辆或者人群的移动方向。

1.4.2　环境监测

无线传感网应用于环境监测，能够完成传统系统无法完成的任务。环境监测应用领域包括：植物生长环境、动物活动环境、生化监测、山体滑坡监测、森林火灾监测、洪水监

测、地震监控等。

我国幅员辽阔，物种众多，环境和生态问题严峻。无线传感网可以广泛地应用于生态环境监测、生物种群研究、气象和地理研究、洪水、火灾检测。一些常见的应用领域如下：

（1）可通过跟踪珍稀鸟类、动物和昆虫的栖息、觅食习惯等进行濒临种群的研究等。

（2）可在河流沿线分区域布设传感器节点，随时监测水位及相关水资源被污染的信息。

（3）在山区中泥石流、滑坡等自然灾害容易发生的地方布设节点，可提前发出预警，以便做好准备，采取相应措施，防止进一步的恶性事故的发生。

（4）可在重点保护林区铺设大量节点随时监控内部火险情况，一旦有危险，可立刻发出警报，并给出具体方位及当前火势大小。

（5）布放在地震、水灾、强热带风暴灾害地区，边远或偏僻野外地区，用于紧急和临时场合应急通信。

2005年，澳大利亚的科学家利用无线传感网来探测北澳大利亚蟾蜍的分布情况。由于蟾蜍的叫声响亮而独特，因此利用声音作为检测特征非常有效。科研人员将采集到的信号在节点上就地处理，然后将处理后的少量结果数据发回给控制中心。通过处理，就可以大致了解蟾蜍的分布、栖息情况。

加州大学在南加利福尼亚San Jacinto建立了可扩展的无线传感网系统，主要监测局部环境条件下小气候和植物甚至动物的生态模式。监测区域（$25hm^2$）分为100多个小区域，每个小区域包含各种类型的传感器节点，该区域的网关负责传输数据到基站，系统由多个网关，经由传输网络到Internet互联网。

加州大学伯克利分校利用部署于一颗高70m的红杉树上的无线传感器系统来监测其生存环境，节点间距2m，监测周围空气温度、湿度、太阳光强（光合作用）等变化。

利用无线传感网系统监测牧场中牛的活动，目的是防止两头牛相互争斗。系统中节点是动态的，因此要求系统采用无线通信模式和高数据速率。

在印度西部多山区域监测泥石流部署的无线传感网系统，目的是在灾难发生前预测泥石流的发生，采用大规模、低成本的节点构成网络，每隔预定的时间发送一次山体状况的最新数据。Intel公司在美国俄勒冈州的一个葡萄园中部署了监测其环境微小变化的无线传感网。

香港由于存在大量山地地貌，城市居民人口众多，要求土地必须保持较高的利用率，因此大量建筑和道路都位于山区附近。由于地处中国南方，地理位置决定了该地区降雨量常年偏高，尤其在每年夏季的梅雨季节，会出现大量的降水。不稳定的山地地貌在受到雨水侵蚀后，容易产生山体滑坡现象，对居民生命财产安全造成巨大的威胁。

过去数十年内在某些极其危险地域发生了多次山体滑坡现象，因此香港政府部门试图部署一种灵活稳定的系统对山体滑坡进行监测和预警。该市政府部门尝试部署过多套有线方式的监测网络，但是由于监测区域往往为人迹罕至的山间，缺乏道路，野外布线、电源供给等都受到限制，使得有线系统部署起来非常困难。此外有线方式往往采用就近部署Datalogger的方式记录采集数据，需要专人定时前往监测点下载数据，系统得不到实时数据，灵活性较差。

地理监测专家进行多次交流，并进行数次实地考察后，地质专业公司在香港青山和大屿山地区部署了基于无线传感网的山体滑坡监测方案。

山体滑坡的监测主要依靠两种传感器的作用，即液位传感器和倾角传感器的作用。在山体容易发生危险的区域，将会沿着山势走向竖直设置多个孔洞。

每个孔洞都会在最下端部署一个液位传感器，在不同深度部署数个倾角传感器。由于该地区的山体滑坡现象主要是由雨水侵蚀产生的，因此地下水位深度是标识山体滑坡危险度的第一指标。该数据由部署在孔洞最下端的液位深度传感器采集并由无线网络发送，如图 1-10 所示。

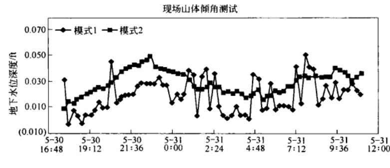


图 1-10　倾角数据

通过倾角传感器可以监测山体的运动状况，山体往往由多层土壤或岩石组成，不同层次间由于物理构成和侵蚀程度不同，其运动速度不同。发生这种现象时我们部署在不同深度的倾角传感器将会返回不同的倾角数据，如图 1-10 所示。在无线网络获取到各个倾角传感器的数据后，通过数据融合处理，专业人员就可以据此判断出山体滑坡的趋势和强度，并判断其威胁性大小。

山体滑坡在地震之后的灾区随处可见，尤其是交通要道两侧的山体滑坡对救援进度更是会造成巨大的威胁，相信无数人仍然记得在听到理县到汶川的生命线在打通后不到一天的时间就又因山体滑坡而中断时那揪心的感觉。

地震是由地壳变化释放能量在地表形成机械波传递的现象。因此安置在地表的振动传感器可以用来检测地震的发生和强度。汶川的地震强度 8 级以及后续的各次余震都是通过地震局汇聚部署在各地的振动传感器信息，再还原为地震中心点的振动数据。

当然长期的地震监测网络，由于其部署地点确定，使用有线监测方式是较为合适的选择。但是在应急情况下，可以随时部署获取数据的无线地震监测网络也具有相当重要的意义。比如在地震之后用以监测余震的发生，机械波的传递远远慢于无线电波，因此可以抢出宝贵的几分钟预警时间给救援人员后撤。

美国哈佛大学在去年部署了一套类似的应急地震监测系统，主要部署在火山地区用来检测因火山爆发而导致的地震信息。

系统采用 TelosB 无线传感器节点，搭载 24 位 ADC 用以监测 MEMS 加速度计传送的微弱振动信息。节点以火山口为中心径向部署，间隔数百米部署一个节点。在部署完毕后可以检测出地震沿径向传播各点的振动信息。

节点在本地进行检测，一旦判断出超过预设门限的振动信息立即发送报警信息，同时通知所有节点开始采集振动波形。所有节点的振动数据会被传送回监控中心，用以进行数学建模还原地震波传递情况。

类似的系统在余震监测和震后应急补充部署时将具有重要的意义。中国地震局、哈尔滨工程力学研究所、中国台湾地震研究中心在近年都开始进行类似项目的研究。期待可以看到在不远的将来能有类似装备问世。

1.4.3 建筑监测

无线传感网用于监测建筑物的健康状况，不仅成本低廉，而且能解决传统监测布线复杂、线路老化、易受损坏等问题。

显而易见在地震中，对人民生命财产安全造成最大伤害的就是建筑物的倒塌。而现今大都市中，摩天大楼林立，在汶川大地震中，北京地区也有震感，华贸、国贸等高层写字楼均有晃动，大量人员有不适感，但直至通过广播、网络确认地震发生后，写字楼人员方开始撤离。如果震中发生在北京附近，这几分钟的迟疑就会带来高层写字楼数千生命的消逝，而北京至少拥有数百栋高层写字楼。

加速度计依然是监测建筑物的最简单有效方式，如图 1-11 所示。美国加州大学伯克利分校对旧金山金门大桥部署过建筑健康监测系统。其本意是用来检测桥体在风力作用下的各个关键受力点的振动状况，整体数据建模后就可以分析出桥体受损老化严重的部分从而进行有针对性的修补。

桥体和高层建筑有一个共同的特点，就是建筑结构及其敏感，因此其前端的测量点部

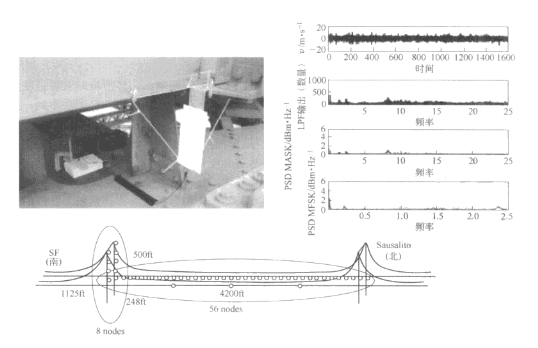


图 1-11 监测建筑物

署很难采用有线方式，否则极易损害建筑结构受力。而无线技术，特别是不需供电的低功耗无线技术，在解决建筑物健康监测前端 100m 数据获取中具有极其重大的意义。节点具有无线能力，体积较为小巧，可以很容易地安装在建筑物的关键受力点上，而不影响建筑物外观。具有低功耗能力，节点一经部署不需要频繁更换。省去了复杂耗时的布线操作，只要打开节点开关，位于建筑物监控中心的接收终端就可以实时获取数据，与建筑报警系统联动后，一旦探测到可能威胁到建筑物的震动信息，立即发出报警通知建筑物内人员立即撤离。平时该系统收集的数据还可以用来监测建筑物老化状况，为建筑物维护提供辅助决策信息。

哈尔滨工业大学欧进萍院士领导的研究团队建立了实验室，专门针对建筑物健康监测进行研究。相关研究成果已经在国内数座桥梁的维护工作中得到应用。

斯坦福大学提出了基于无线传感网的建筑物监测系统，采用基于分簇结构的两层网络系统。传感器节点由 EVK915 模块和 ADXL210 加速度传感器构成，簇首节点由 Proxim RangelLAN2 无线调制器和 EVK915 连接而成。

南加州大学开发了一种监测建筑物的无线传感网系统 NETSHM，该系统除了监测建筑物的健康状况外，还能够定位出建筑物受损伤的位置。系统部署于 Los Angeles 的 The Four Seasons 大楼内。系统采用分簇结构，采用 Mica-Z 系列节点。

对珍贵的古老建筑进行保护，是文物保护单位长期以来的一个工作重点。将具有温度、湿度、压力、加速度、光照等传感器的节点布放在重点保护对象当中，无需拉线钻孔，便可有效地对建筑物进行长期的监测。此外，对于珍贵文物而言，在保存地点的墙角、天花板等位置监测环境的温度、湿度是否超过安全值，可以更妥善地保护展览品的品质。

1.4.4 医疗卫生

无线传感网在检测人体生理数据、老年人健康状况、医院药品管理以及远程医疗等方面可以发挥出色的作用。在病人身上安置体温采集、呼吸、血压等测量传感器，医生可以远程了解病人的情况。利用传感器网络长时间地收集人的生理数据，这些数据在研制新药品的过程中非常有用。

美国英特尔公司目前正在研制家庭护理的无线传感网系统。该系统是美国“应对老龄化社会技术项目”的一个环节。根据演示，该系统在鞋、家具以及家用电器等中嵌入传感器，帮助老年人及患者、残障人士独立地进行家庭生活，并在必要时由医务人员、社会工作者进行帮助。

研究人员开发出基于多个加速度传感器的无线传感网系统，用于进行人体行为模式监测，如坐、站、躺、行走、跌倒、爬行等。该系统使用多个传感器节点，安装在人体几个特征部位。系统实时地把人体因行动而产生的三维加速度信息进行提取、融合、分类，进而由监控界面显示受检测人的行为模式。这个系统稍加产品化，便可成为一些老人及行动不便的病人的安全助手。同时该系统也可以应用到一些残障人士的康复中心，对病人的各类肢体恢复进展进行精确测量，从而为设计复健方案带来宝贵的参考依据。

研究人员可以利用无线传感网来实现远程医疗监视。在一个公寓内 17 个传感器节点分布在各个房间，包括卫生间。每个传感器节点上包括了温度、湿度、光、红外传感器及

声音传感器，部分节点使用了超声节点。根据这些节点收集到的信息，监控界面实时显示人员的活动情况。根据多传感器的信息融合，可以相当精确地判断出被检测人正在进行的行为，例如做饭、睡觉、看电视、淋浴等等，从而可以对老年人健康状况，如老年痴呆症等进行精确检测。因为系统不使用摄像机，比较容易得到病人及其家属的接受。

加利福尼亚大学提出了基于无线传感网的人体健康监测平台 CustMed，采用可佩戴的传感器节点，传感器类型包括压力、皮肤反应、伸缩、压电薄膜传感器、温度传感器等。节点采用加州大学伯克利分校研制的 dot-mote 节点，通过放在口袋里的 PC 机可以方便直观地查看人体当前的情况。

纽约 Stony Brook 大学针对当前社会老龄化的问题提出了监测老年人生理状况的无线传感网系统（Health Tracker 2000），除了监测用户的生理信息外，还可以在生命发生危险的情况下及时通报其身体情况和位置信息。

1.4.5 智能交通

上海市重点科技研发计划中的智能交通监测系统，采用声音、图像、视频、温度、湿度等传感器，节点部署于十字路口周围，部署于车辆上的节点还包括 GPS 全球定位设备。重点强调了系统的安全性问题，包括耗能、网络动态安全、网络规模、数据管理融合、数据传输模式等。

1995 年，美国交通部提出了到 2025 年全面投入使用的“国家智能交通系统项目规划”。该计划利用大规模无线传感网，配合 GPS 定位系统等资源，除了使所有车辆都能保持在高效低耗的最佳运行状态、自动保持车距外，还能推荐最佳行使路线，对潜在的故障可以发出警告。

中国科学院沈阳自动化所提出了基于无线传感网的高速公路交通监控系统，节点采用图像传感器，在能见度低、路面结冰等情况下，能够实现对高速路段的有效监控。

1.4.6 农业领域

我国是农业大国，农作物的优质高产对国家的经济发展意义重大。在这些方面，无线传感网有着卓越的技术优势。它可用于监视农作物灌溉情况、土壤空气变更、牲畜和家禽的环境状况以及大面积的地表检测。

一个典型的系统通常由环境监测节点、基站、通信系统、互联网以及监控软硬件系统构成。根据需要，人们可以在待测区域安放不同功能的传感器并组成网络，长期大面积地监测微小的气候变化，包括温度、湿度、风力、大气、降雨量，收集有关土地的湿度、氮浓缩量和土壤 pH 值等，从而进行科学预测，帮助农民抗灾、减灾，科学种植，获得较高的农作物产量。在“九五”计划中，“工厂高效农业工程”已经把智能传感器和传感器网络化的研制列为国家重点项目。以下介绍国内外在这个领域所作的一些尝试。

2002 年，英特尔公司率先在俄勒冈建立了世界上第一个无线葡萄园。传感器节点被分布在葡萄园的每个角落，每隔一分钟检测一次土壤温度、湿度和该区域有害物的数量，以确保葡萄可以健康生长。研究人员发现，葡萄园气候的细微变化可极大地影响葡萄酒的质量。通过长年的数据记录以及相关分析，便能精确地掌握葡萄酒的质地与葡萄生长过程中的日照、温度、湿度的确切关系。这是一个典型的精准农业、智能耕种的实例。

北京市科委计划项目“蔬菜生产智能网络传感器体系研究与应用”正式把农用无线传感网示范应用于温室蔬菜生产中。在温室环境里单个温室即可成为无线传感网的一个测量控制区，采用不同的传感器节点构成无线网络来测量土壤湿度、土壤成分、pH 值、降水量、温度、空气湿度和气压、光照强度、CO_2 浓度等，获得农作物生长的最佳条件，为温室精准调控提供科学依据。最终使温室中传感器、执行机构标准化、数字化、网络化，从而达到增加作物产量、提高经济效益的目的。

无线传感网通信便利、部署方便的优点使其在节水灌溉的控制中得以应用。同时，节点还具有土壤参数、气象参数的测量能力，再与互联网、GPS 技术结合，可以比较方便地实现灌区动态管理、作物需水信息采集与精量控制专家系统的构建，并可进而实现高效、低能耗、低投入、多功能的农业节水灌溉平台。可在温室、庭院花园绿地、高速路隔离带、农田井用灌溉区等区域，实现农业与生态节水技术的定量化、规范化、模式化、集成化，促进节水工业的快速和健康发展。

Digital Sun 公司发展的自动洒水系统 S. Sense Wireless Sensor 目前受到国际上多家媒体的报道。它使用无线传感器感应土壤的水分，并在必要时与接收器通信，控制灌溉系统阀门的打开和关闭，从而达到自动、节水灌溉的目的。

西北农林科技大学的教授认为，无线传感网的诸多优势，特别适用于以下方面的生产和科学研究，例如，大棚种植室内及土壤的温度、湿度、光照监测、珍贵经济作物生长规律分析与测量、葡萄优质育种和生产等，可为许多杨凌示范区内农村发展与农民增收项目带来高科技的辅助手段。此外，该项技术还为贵重药材生长条件检测与模拟、果园、高经济价值作物的生长条件分析与人工干预、林业防火防盗等提供有力手段。

陕西秦巴山区的许多珍贵药材的生长规律，可以通过该项技术得到精确测量，通过无线信道、卫星或互联网传输到控制中心，从而可以精确掌握这类药材的生长周期、水分、湿度、光照、雨水等资料。根据分析结果，农业人员就可以在人造环境下进行逼真的模拟，有望提高产量、改善稀有药材紧缺的现状。

采用无线传感网建设农业环境自动监测系统，用同一套网络分别完成风、光、水、电、热和农药等的数据采集和环境控制，可有效提高农业集约化生产程度，简化系统复杂性，降低设备成本。

1.4.7 工业领域

英国石油公司总裁卡萨尔称，传感器网络可用于危险工作环境，在煤矿、石油钻井、核电厂和组装线工作的员工将可以得到随时监控。这些传感器网络可以告诉工作现场有哪些员工、他们在做什么以及他们的安全保障等重要信息。在相关的工厂每个排放口安装相应的无线节点，完成对工厂废水、废气污染源的监测，样本的采集、分析和流量测定。“无线传感网技术几乎在我们的各项业务中都将得到应用。我们不会仅停留在几十只或几百只的使用规模。最终，这个数字将会数以万计。”

煤矿、石化、冶金行业对工作人员安全，易燃、易爆、有毒物质监测的成本一直居高不下，无线传感网把部分操作人员从高危环境中解脱出来的同时，提高了险情的反应精度和速度。

我国大型煤矿六百多家，中型煤矿两千多家，中小型煤矿一万余家。煤炭行业对先进

的井下安全生产保障系统的需求巨大。陕西彬长矿区的孙斌建高工认为，无线传感网对运动目标的跟踪功能、对周边环境的多传感器融合监测功能，使其在井下安全生产的诸多环节有着很大的发展空间。

北京邮电大学的研究人员开展了煤矿瓦斯报警和矿工定位无线传感网系统的研究，一个节点上包括了温湿度传感器、瓦斯传感器、粉尘传感器等。传感器网络经防爆处理和技术优化后，可用于危险工作环境，在煤矿工作的员工及其周围环境将可以得到随时监控。

陕西天和集团研发矿工井下区段定位系统，其结构框图如图 1-12 所示。各个工作地点放置一定数量的传感器节点，通过接收矿工随身携带的节点所发射的具有唯一识别码的无线信号进行人员定位。同时各个传感器节点还可以进行温度、湿度、光、声音、风速等参量的实时检测，并将结果传输至基站，进而传至管理中心。

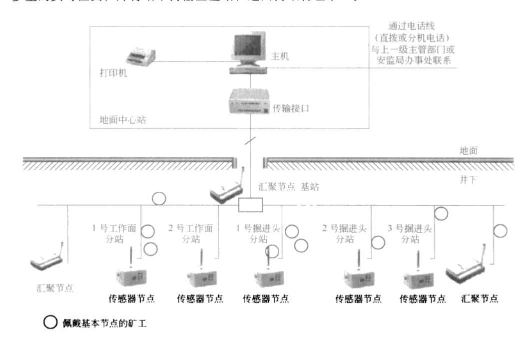


图 1-12 矿工井下区段定位

随着制造业技术的发展，各类生产设备越来越复杂精密。现在工作人员从生产流水线到复杂机器设备，都尝试着安装相应的传感器节点，以便时刻掌握设备的工作健康状况，及早发现问题及早处理，从而有效地减少损失，降低事故发生率。

电子科技大学、中国空气动力研究与发展中心以及北京航天指挥控制中心的研究人员，利用无线传感网进行大型风洞测控环境的监测，对旋转机构，气源系统、风洞运行系统以及其他没有基础设施而有线传感器系统安装又不方便或不安全的应用环境进行全方位检测。

美国英特尔公司为俄勒冈的一家芯片制造厂安装了 200 台无线传感器，用来监控部分工厂设备的振动情况，并在测量结果超出规定时提供监测报告。英特尔研究中心的主管助理汉斯·穆德尔说，这项计划目前虽然只涵盖了工厂 4000 种可测部件中的少数部件，但

是效果却非常显著。如今，研究人员再也不需要每隔两三个月就到每台机器处来回巡视了。

我国高科技企业林立，在诸如集成电路芯片生产、大型精密设备状态监测等方面有着巨大的技术需求和市场，无线传感网技术在这些领域将大有作为。

除了上述提到的应用领域外，无线传感网还可以应用于安防系统、智能家居、仓库物流管理、空间海洋探索、资源勘探、污染监控、灾难预防等领域。

1.5 无线传感网面临的技术挑战

无线传感网是一种独立出现的计算机网络，它的基本组成单位是节点，这些节点集成了传感器、微处理器、无线接口和电源四个模块。传统的计算机网络技术中业已成熟的解决方案可以借鉴到无线传感网中来。但是基于无线传感网自身的用途和优点，开发专用的通信协议和路由算法已经成为了当前无线传感网领域内急待研究的课题，如 ZigBee 无线网络国际通信标准。

1.5.1 通信距离

在将无线传感网应用到野外时最大的问题是如何保证节点在重植被覆盖下仍能正常组网通信。容易发生地质灾害的山区往往植被密集，在进行项目（环境非常类似山区，人迹罕至，高达一人高的野草和大量树木）之前数次派人进行实地考察，并进行了详细的讨论和分析，最终 2.4GHz 被认为最为适合该环境的使用。

由表 1-1 可以看出，重植被与暴雨都会对无线信号产生衰减。433MHz 由于其波长较长，因此绕射性能较好，在雨中具有较好的表现。2.4GHz 由于波长较短，穿透性较好，在重植被环境下具有较好的表现。重植被造成的衰减为暴雨的数千倍，且系统工作在降雨环境下的时间应该在 50% 以下。因此 2.4GHz 应该更适合野外环境的使用。

表 1-1 重植被与暴雨都会对无线信号产生衰减

环 境	衰 减	环 境	衰 减
暴雨（101.6mm/h）	0.05dB/km（0.08dB/mile）	植 被	2dB/m
倾盆大雨	0.1dB/km	灌木林	3-4dB/m
浓 雾	0.02dB/km（0.03dB/mile）	针叶林	8-10dB/m
少量树木	0.3～0.5dB/m	森 林	300dB/km

此外考虑频谱环境，目前使用 2.4GHz 的商用设备如 Wi-Fi、BlueTooth 多为短距设备，因此 2.4GHz 频段较为干净，干扰较少。400MHz 与 900MHz 的干扰则相对较多。在地质灾害发生时，大量使用的单兵电台，步话机等极其容易造成相互干扰。从避免干扰的角度来说，2.4G 是较佳的选择。

尽管 2.4GHz 具有相对较好的表现，重植被和降雨仍然会对无线信号产生较大的衰减。现代传感器节点，由于采用了全新的芯片组以及模块化设计生产。在通信距离指标上得到大幅提高，同时其功耗反而得到一定降低。

在北京地区进行的湖面环境测试时，该节点达到了 1000m 的通信距离。在换装 5dBi 增益天线后，节点在北京二环路上下班高峰时期的车辆密集情况下也达到了 500m 的通信

距离。而其功耗相对原有的节点降低了1/3左右。

1.5.2 能源消耗

无线传感网应用于特殊场合时，电源不可更换，因此功耗问题显得至关重要。

在系统的功耗模型中，最关心的问题是：

(1) 微控制器的操作模式（休眠模式、操作模式、潜在的减慢时钟速率等），无线前端的工作模式（休眠、空闲、接收、发射等）；

(2) 在每种模式中，每个功能块的功耗量以及它与哪些参数有关；

(3) 在发射功率受限的情况下，发射功率和系统功耗的映射关系；

(4) 从一种操作模式转换到另外一种操作模式（假设可以直接转换）的转换时间及其功耗；

(5) 无线调制解调器的接收灵敏度和最大输出功率；

(6) 附加的品质因数（如发射前端的温漂和频稳度、接收信号场强指示（RSSI）信号的标准等）。

每个节点通过电池供电，在电源管理机制下，能够提供更加优异的电量表现，电池电量能维持节点连续工作几个月到几年以上。

电池的电压随时被监控，一旦电压过低，节点会将电压数据发至基站。这个数据发送成功后，节点会处于深度睡眠模式，管理者在获得了某个节点电压过低的警告后，就可以有目的地进行系统的维护工作。当这个节点被重新换上新电池后将自动正常工作。

1.5.3 可靠通信

无线传感网被布置在无人值守的环境中时，更换能源几乎不可能，为了节约能源，发射功率要尽可能小，传输距离要短，节点间通信需要中间节点作为中继。

在地震救灾或者是无人飞行器中，网络的自动配置和自动康复功能显得异常重要，而大规模的多跳无线传感网系统的可测量性（scalability）也是一个关键问题。实现可测量性的一种方法是"分而治之（divide and conquer）"，或者说是分层控制（hierarchical），即用某种簇标准将网络节点分成簇组（clusters），在每个簇中选出一个作为簇头（leader），它在比较高的层次上代表本簇；同样的机制也应用到簇头中，使之形成一个层次，这个层次中，每个级别应用当地控制（local control）去实现某个全局目标。

大多数无线网络中的分类思想认为网络与地理位置无关，分类的标准是簇里的节点数量和簇间的逻辑直径（相对于地理直径而言）。但是当簇头（cluster leader）和簇内其他节点间的链路很长，相邻簇间地理位置交叠很大，且不同的簇间路由消息载荷（routing traffic load）不平衡时，一个非簇头（non-leader）节点和它的簇头节点之间通过它们之间仅有的长链路通信将要消耗更多的能量，并且相邻簇间的并行通信冲突频发，簇间能量消耗不平衡，由此带来的结果是网络的寿命和通信质量与有效性都大幅度减小。

因此为了节约能量和改善通信质量和有效性，在设计簇算法时，簇的地理半径应该考虑。在传感器节点内用一种简单的细胞聚类结构去构成路由协议，这样可以维持一种可测量的能量有效的系统，其关键的问题是使这种细胞簇结构具有自动康复性。

针对大规模多跳传感器网络的自动配置和自动康复提出了一种分布式算法，这种算法

可以保证网络节点在二维空间里自动配置成细胞簇结构，其细胞单元有紧凑的地理半径，细胞单元之间的交叠也很小。这种结构在各种扰动下是自动康复的，比如节点加入、离开、死亡、移动、被敌方捕获等。

一种针对簇的分布式算法 LEACH，它是通过全局上重复簇操作来处理扰动的，但这种算法既不能保证系统中簇的定位也不能保证簇的数量。

另外一种簇算法，它仅考虑了簇的逻辑半径，而不考虑地理半径，当簇间存在比较大的交叠时，这种方法会降低无线传输的有效性。另外它的康复不在本地处理，而是依赖于消息在整个系统中的多次循环。

一种基于访问的簇算法，这种算法注重簇的稳定性，不考虑簇的大小，要求每个节点都有全球定位系统（GPS）的支持。

无线通信都存在一定的数据丢失率，用在环境监测中时，丢失一次采集信息并不会对全局的海量数据造成任何影响。但是当用在地质灾害监测中时，它所传递的信息关系重大，一旦丢失所造成的影响极其严重。端到端的发送信息确认，专门用以发送确认数据包，在该模式下每个数据包在经过多跳传输到达目的节点后，目的节点会立刻回传一个 ACK 数据包，发送端在经过确定时间延时（根据路由表跳数确定）没有收到 ACK 数据包，会立刻重新发送，重复该过程直到数据包安全到达目的地。

1.5.4　网络安全

传感器网络受到的安全威胁和移动网络所受到的安全威胁不同，所以现有的网络安全机制不适合此领域，需要开发针对无线传感网的专门协议，如图 1-13 所示。

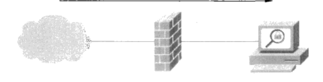


图 1-13　网络安全

一种思想是从维护路由安全的角度出发，寻找尽可能安全的路由以保证网络的安全。如果路由协议被破坏导致传送的消息被篡改，那么对于应用层上的数据包来说没有任何的安全性可言。

一种方法叫“有安全意识的路由”（SAR），其思想是找出真实值和节点之间的关系，然后利用这些真实值去生成安全的路由。该方法解决了两个问题，即如何保证数据在安全路径中传送和路由协议中的信息安全性。假设两个军官利用按需距离矢量路由（Ad Hoc On Demand Distance Vector Routing，AODV）协议通过 ad hoc 网络来通信，他们的通信基于 Bell-La 安全模型（Padula Bell-La Padula Confidentiality Model），这种模型中，当节点的安全等级达不到要求时，其就会自动地从路由选择中退出以保证整个网络的路由安全。

可以通过多径路由算法改善系统的稳健性（robustness），数据包通过路由选择算法在多径路径中向前传送，在接收端内通过前向纠错技术得到重建。

无线传感网中传感器的数量众多并且功能有限，移动 ad hoc 网络中的路由方案不能直

接应用到无线传感网中，所以该文给出了一种网状多径路由协议。此协议中应用了选择性向前传送数据包和端到端的前向纠错解码技术，配合适合传感器网络的网状多径搜索机制，能减少信号开支（signaling overhead），简化节点数据库，增大系统的吞吐量，相对数据包复制或者有限泛洪法来说，这种方法消耗更少的系统资源（比如信道带宽和电能）。

另一种思想是把着重点放在安全协议方面，在此领域也出现了大量的研究成果。假定传感器网络的任务是为高级政要人员提供安全保护，提供一个安全解决方案将为解决这类安全问题带来一个普适的模型。在具体的技术实现上，先假定基站总是正常工作的，并且总是安全的，满足必要的计算速度、存储器容量，基站功率满足加密和路由的要求；通信模式是点到点，通过端到端的加密保证了数据传输的安全性；射频层总是正常工作。基于以上前提，典型的安全问题可以总结为：

（1）信息被非法用户截获；

（2）一个节点遭破坏；

（3）识别伪节点；

（4）如何向已有传感器网络添加合法的节点。

提出的方案不采用任何的路由机制。在此方案中每个节点和基站分享一个唯一的 64 位密匙 Keyj 和一个公共的密匙 KeyBS，当节点和基站距离超出了预定距离时，网络会在节点和基站之间选择一个节点作为媒介节点进行接力；发送端会对数据进行加密，接收端接收到数据后根据数据中的地址选择相应的密匙对数据进行解密。这种双加密方式可以防止暴露节点数目和地址，也可以防止数据被非法截获，即使个别节点被破译，也只有它自己的密匙泄漏，整个网络仍然可以正常工作。

无线传感网有两种专用安全协议，即 SNEP（Sensor Network Encryption Protecol）和 TESLA。SNEP 的功能是提供节点到接收机之间数据的鉴权、加密、刷新，TESLA 的功能是对广播数据的鉴权。

1.6 无线传感网的未来

无线传感网有着十分广泛的应用前景，它不仅在工业、农业、军事、环境、医疗等传统领域具有巨大的运用价值，在未来还将在许多新兴领域体现其优越性，如家用、保健、交通等领域。我们可以大胆地预见，将来无线传感网将无处不在，将完全融入我们的生活。比如微型传感器网最终可能将家用电器、个人电脑和其他日常用品同互联网相连，实现远距离跟踪，家庭采用无线传感网负责安全调控、节电等。无线传感网将是未来的一个无孔不入的十分庞大的网络，其应用可以涉及人类日常生活和社会生产活动的所有领域，如图 1-14 所示。

据 B&B Electronics 和 Sensicast Systems 进行的一项在线调查显示，在 200 家工业终端用户及系统集成商中，有超过 50% 的公司正考虑在未来配置无线传感网。与此对应，也有一个类似的调查，结果则显示有 45% 被调查者计划在今后三年内配置无线传感网。此外该调查还显示，2.4GHz 工作频率最受青睐，在早些时候的调查中，选择 2.4GHz 的被调查者人数是选择 900MHz 的两倍。这次的研究结果显示，被调查者中，对无线传感网络特别是工业监控感兴趣的人数在持续增长，有 73% 的被调查者在研究无线网络在该领域中的应用。

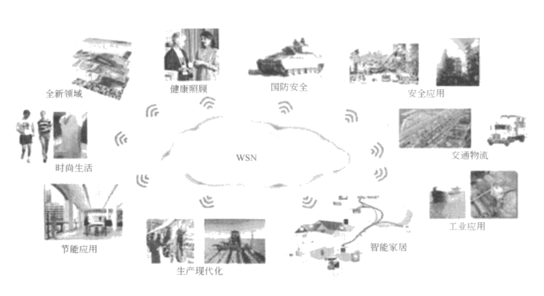


图 1-14 无线传感网的应用

2003 年，美国《技术评论》杂志论述最有影响的改变世界的十大技术之时，无线传感网被列为第一项未来新兴技术。同年美国《商业周刊》未来技术专版论述四大新技术时，无线传感网也列入其中。

无线传感网被麻省理工学院（MIT）技术评论列为全球未来的三大高科技产业。

美国《今日防务》杂志更认为无线传感网的应用和发展，将引起一场划时代的军事技术革命和未来战争的变革。2004 年《IEEE Spectrum》杂志发表一期专集——传感器的国度，论述无线传感网的发展和可能的广泛应用。可以预计，无线传感网的发展和广泛应用，将对人们的社会生活和产业变革带来极大的影响和产生巨大的推动。

在一份我国未来 20 年预见技术的调查报告中，信息领域 157 项技术课题中有 7 项与传感器网络直接相关。2006 年初发布的《国家中长期科学与技术发展规划纲要》为信息技术定义了三个前沿方向，其中两个与 WSN 的研究直接相关，即智能感知技术和自组织网络技术。我国 2010 年远景规划和“十五”计划中将 WSN 列为重点发展的产业之一。

根据无线传感网的研究现状，无线传感网技术的发展趋势主要有以下 4 个方面：

（1）灵活、自适应的网络协议体系。无线传感网广泛地应用于军事、环境、医疗、家庭、工业等领域。其网络协议、算法的设计和实现与具体的应用场景有着紧密的关联。在环境监测中需要使用静止、低速的无线传感网；军事应用中需要使用移动的、实时性强的无线传感网；智能交通里还需要将 RFID 技术和无线传感网技术融合起来使用。这些面向不同应用背景的无线传感网所使用的路由机制、数据传输模式、实时性要求以及组网机制等都有着很大的差异，因而网络性能各有不同。目前无线传感网研究中所提出的各种网络协议都是基于某种特定的应用而提出的，这给无线传感网的通用化设计和使用带来了巨大的困难。如何设计功能可裁减、自主灵活、可重构和适应于不同应用需求的无线传感网协议体系结构，将是未来无线传感网发展一个重要方向。

（2）跨层设计。无线传感网有着分层的体系结构，因此在设计时也大都是分层进行

的。各层的设计相互独立且具有一定局限性，因而各层的优化设计并不能保证整个网络的设计最优。针对此问题，一些研究者提出了跨层设计的概念。跨层设计目标就是实现逻辑上并不相邻的协议层之间的设计互动与性能平衡。对无线传感网，能量管理机制、低功耗设计等在各层设计中都有所体现；但要使整个网络的节能效果达到最优，还应采用跨层设计思想。

将MAC与路由相结合进行跨层设计可以有效节省能量，延长网络的寿命。同样，传感器网络的能量管理和低功耗设计也必须结合实际跨层进行。此外，在时间同步和节点定位方面，采用跨层优化设计的方式，能够使节点直接获取物理层的信息，有效避免本地处理带来误差，获得较为准确的相关信息。

（3）ZigBee标准规范。ZigBee是一种新兴无线网络通信规范，主要用于近距离无线连接。ZigBee的基础是IEEE无线个域网工作组所制定的IEEE802.15.4技术标准口。802.15.4标准旨在为低能耗的简单设备提供有效覆盖范围在10m左右的低速连接，可广泛用于交互玩具、库存跟踪监测等消费与商业应用领域。ZigBee当然不仅只是802.15.4的名字。IEEE802.15.4仅处理低级MAC层和物理层协议，ZigBee联盟对其网络层协议和API进行了标准化，还开发了安全层，以保证这种便携设备不会意外泄漏其标识，而且这种利用网络的远距离传输不会被其他节点获得。此外ZigBee还具有低传输速率、低功耗、协议简单、时延短、安全可靠、网络容量大、优良的网络拓扑能力等优点。ZigBee的这些优点极好地支持了无线传感网：它能够在众多微小的传感器节点之间相互协调实现通信，这些节点只需要很低的功耗，以多跳接力的方式在节点间传送数据，因而通信效率非常高。目前，ZigBee联盟正在进行协议标准的整合工作，该标准的成功制定对于无线传感网的推广使用将有着深远、重要的意义。

（4）与其他网络的融合。无线传感网和现有网络的融合将带来新的应用。例如，无线传感网与互联网、移动通信网的融合，一方面使无线传感网得以借助这两种传统网络传递信息，另一方面这两种网络可以利用传感信息实现应用的创新。此外，将无线传感网作为传感与信息采集的基础设施融合进网格体系，构建一种全新的基于无线传感网的网格体系——无线传感网。传感器网络专注于探测和收集环境信息；复杂的数据处理和存储等服务则交给网格来完成，将能够为大型的军事应用、科研、工业生产和商业交易等应用领域提供一个集数据感知、密集处理和海量存储于一体的强大操作平台。

第2章　现代无线传感网开发环境

国内目前在现代无线传感网软件、硬件方面也取得了相应的突破，在基于国际标准、操作系统之上，已开发出了自己的硬件平台、中间件软件。如南京邮电大学无线传感网研究中心开发的基于移动代理的无线传感网中间件平台；无线龙科技 C51RF-WSN 无线传感网开发平台，提供了功能齐全的硬件开发平台，对外提供便捷的接口，使用户无需了解底层细节，极大地降低了无线传感网应用开发的难度。

国内研究机构在理论研究方面，如对无线传感网网络协议、算法、体系结构等方面，提出了许多具有创新性的想法与理论。在这方面，国内的南京邮电大学、哈尔滨工业大学、清华大学、上海交通大学、北京邮电大学等都取得了一些相关的理论研究成果。

目前国内比较成功的无线传感网软件产品包括：南京邮电大学的无线传感网中间件软件，南京邮电大学的无线传感网集成开发平台，无线龙科技 C51RF-WSN 现代无线传感网开发平台及中间件，中国科学院无线传感网分析与管理平台。

现代无线传感网开发平台 C51RF-WSN 由计算机部分、网关部分、网络节点部分等三部分组成，用户可以很方便地实现传感器网络的无线化、网络化、规模化演示，观测和再次开发。

（1）计算机部分。完成接收网关数据和发送指令，实现可视化、形象化人机界面，方便用户操作、观察。

（2）网关部分。完成通过计算机发送的指令，发送或接收路由节点或者传感器节点数据，并将接收到的数据发送给计算机。

（3）网络节点部分。网络节点包括两大功能：1）在网关不能和所有的传感器节点通信时，路由节点作为一种中介使网关和传感器节点通信，实现路由通信功能；2)完成对设备的控制和数据的采集,例如灯的控制,温度数据、光照度数据等的采集。

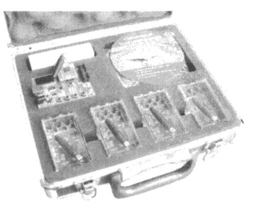


图 2-1　探索系列 EXPLORERF-MC13224 无线传感器实验平台

现代无线传感网开发、实验平台 C51RF-WSN 系列平台根据不同通信协议标准、不同控制器、不同无线节点包括如下型号：C51RF-WSN-CC2430、C51RF-WSN-CC2520、EXPLORERF-MC13224（见图 2-1）、EXPLORERF-CC2530、EXPLORERF-CC2430、DREAMRF-CC2430、DREAMRE

CC2530 等。

2.1 无线传感网系统构架

现代无线传感网开发、实验平台 C51RF-WSN 根据不同的情况可以由一台计算机、一套网关、一个或多个网络节点组成。系统大小只受 PC 软件观测数量、路由深度、网络最大负载量限制。

现代无线传感网开发、实验平台 C51RF-WSN 内配置 ZigBee2007/PRO、ZigBee2006 等协议栈，在没有进行网络拓扑修改之前支持 5 级路由、31101 个网络节点。传感器网络系统结构如图 2-2 所示。

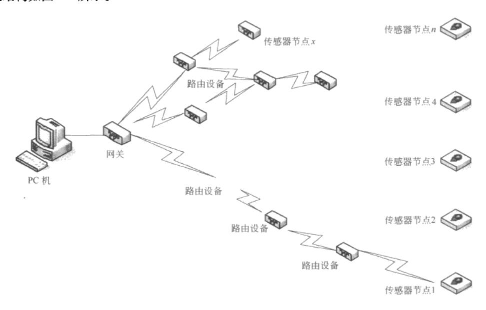


图 2-2 传感器网络系统结构

基于 ZigBee2007/PRO、ZigBee2006 等协议栈的无线传感网具有自组织能力，其在网络设备安装和架设过程中自动完成网络组建。完成网络的架设后用户便可以由 PC 机发出命令读取网络中任何设备上挂接的传感器的数据以及测试其电压。简单的工作流程描述如图 2-3 所示。

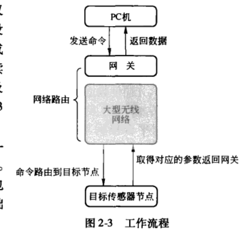


图 2-3 工作流程

在使用现代无线传感网开发平台 C51RF-WSN 前，用户需要学习并理解一些基础知识。顾名思义，现代无线传感器网络实验平台即包括无线数据传输、无线网络、传感器三大基础部分。

2.2 现代无线传感网平台

现代无线传感网开发、实验平台 C51RF-WSN 是精心设计的一款集教学、竞赛、工控开发于一身的无线传感网开发、实验平台。平台以飞思卡尔公司的以 ARM7 为内核 MC13224、TI 公司以 C8051 为内核 CC2430/CC2530、TI 公司以 MSP430 为内核 MSP430F54XX 等为微控制器，支持国际 802.15.4 标准以及 ZigBee、ZigBee PRO 和 ZigBee RF4CE 标准；提供了 90～104dB 的链路质量，优秀的接收器灵敏度和健壮的抗干扰性，多种供电模式，多种传感器，以及一套广泛的外设集——包括高速 UART、8～12 位 ADC 和 32～64 个通用 GPIO，4 个定时器，I2C 等等。除了业界标准 ARM7TDMI-S、C8051 内核，支持低功耗无线通信，改进了 RF 输出功率、灵敏度、选择性，且一般会提供一个超越上一代无线传感网芯片的重要性能改进。

现代无线传感网开发、实验平台 C51RF-WSN 完全满足 IEEE802.15.4 标准和 ZigBee2006/2007/PRO 技术标准的无线网络技术设计开发。该平台除了提供构建多种 ZigBee 网络所需的全部硬件、软件专业开发工具、文档和各种展示、表演软件，还增加无线传感网演示程序，提供最多的资料、最丰富的实验、最完善的技术支持，能帮助用户早日掌握现代无线传感网并完成自己的项目开发。

现代无线传感网开发、实验平台 C51RF-WSN 应用包括远程控制、工业控制、HVAC、卫生保健消费型电子、家庭控制、计量和智能能源、楼宇自动化、医疗以及更多领域。

现代无线传感网开发、实验平台 C51RF-WSN 主要包括 1 套网关、4～8 个网络节点、1～2 台仿真器、1 套可视代上位机监控软件、1 张开发光盘及若干数据线，如图 2-4 所示。

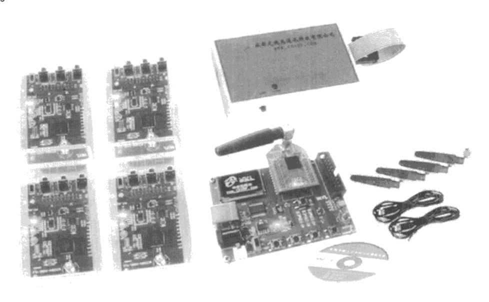


图 2-4 C51RF-WSN

2.2.1 无线传感网平台仿真器

首先我们来看看现代无线传感网开发、实验平台 C51RF-WSN 仿真器，仿真器具有在线下载、调试、仿真等功能。仿真器外形非常简洁，具有一个 USB 接口，一个指示灯以及一根仿真下载线。

（1）USB 接口：通过 USB 接口把仿真器与计算机有机地连接起来。仿真器通过此接口与计算机进行通信，要在无线网络节点模块的开发上实现下载、调试（DEBUG）、仿真等的通信都由此接口来实现。

（2）指示灯：电源指示灯。

（3）仿真线：这是一根下载、调试（DEBUG）仿真线，通过它与无线节点模块或开发板进行连接。

现代无线传感网开发、实验平台 C51RF-WSN 仿真器具有以下特点：

（1）USB 接口，使现代无线传感网开发、实验平台 C51RF-WSN 开发与计算机连接更加简单快捷。

（2）高速代码下载，现代无线传感网开发、实验平台 C51RF-WSN 仿真器提供高速下载速度，把程序下载到无线节点模块只需要几秒就完成。

（3）在线下载、调试、仿真。

（4）硬件断点调试，类似 JTAG 的硬件断点调试，可实现单步、变量（寄存器）观察等全部 C51 源代码水平的在线调试 DEBUG 功能。

（5）支持 IAR 的 C51/ARM 编译/调试图形 IDE 开发平台。

（6）专业设计，系统稳定可靠，噪声干扰小。

2.2.2 无线传感网平台网关

现代无线传感网开发、实验平台 C51RF-WSN 的网关主要由一个底板及一个无线网络节点模块组成，如图 2-5 所示。

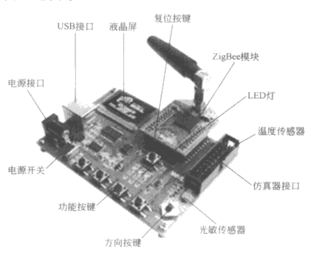


图 2-5 C51RF-WSN 网关

网关节点通过 USB 口和计算机（PC 机）实现通信；通过网关内置无线模块和各无线传感网节点实现通信。网关节点是将所有节点数据汇总、分析、存储和发送的一个机构。

无线传感网平台网关的工作流程是：当计算机发送命令以后，网关接收命令，首先判断是不是可用的命令，如果可用，根据命令判断计算机需要哪个节点的信息，并向该节点发送命令要求将对应数据传回网关，然后再将接收到的指定节点的信息按既定格式发送给 PC 机，PC 机通过传感器网络 PC 软件显示出来。

在 ZigBee2006/2007/PRO 无线网络中，网关起一个 ZigBee 无线网络协调器的作用，负责对 ZigBee 无线网络的管理及维护。

2.2.3 无线传感网平台网络节点

现代无线传感网开发、实验平台 C51RF-WSN 网络节点主要由各种传感器、无线网络芯片、天线、按键、电池盒、扩展接口、仿真器接口、外接电源接口及 LED 指示灯等组成。

现代无线传感网开发、实验平台 C51RF-WSN 网络节点提供电池及外接电源两种供电模式。电池供电模式使用的是两节 5 号电池。外接电源电压要求为 3.0 ~ 3.3V，外接电源时，注意电源正负极性。

网络节点提供了 3 种传感器，包括光敏传感器、温度传感器及三维加速度传感器等，如图 2-6 所示。

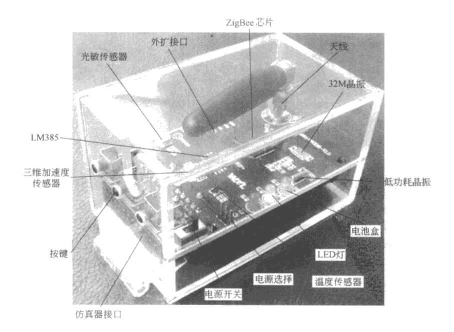


图 2-6 C51RF-WSN 网络节点

网络节点提供 10 个扩展接口，分别是 VCC、SCL、SDA、TX、RX、CTS、RTS、

ADC2、ADC1、GND，如图 2-7 所示。

网络节点提供 1 个 32M 或 24M 正常工作晶振及 1 个低功耗晶振。

网络节点在 ZigBee2006/2007/PRO 无线传感网中负责数据采集及数据的传输。

现代无线传感网开发、实验平台 C51RF-WSN 网络节点根据功能需求可选择充当路由节点或终端节点使用。

J3

引脚	信号
10	VCC
9	I2C_SCL
8	I2C_SDA
7	UART1-TX
6	UART1-RX
5	UART1-CTS
4	UART1-RTS
3	ADC2
2	ADC1
1	GND

CON10

图 2-7 扩展接口

2.2.4 无线节点模块

在网关中配套的无线节点模块采用飞思卡尔或 TI 芯片 MC13224、CC2530、CC2520、CC2430。无线节点模块主要由芯片、晶振、天线、扩展引脚及 LED 灯等组成，如图 2-8 所示。

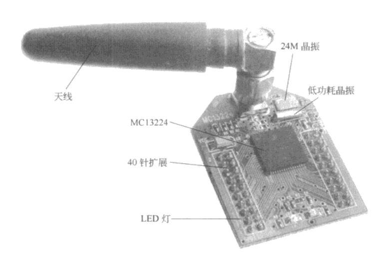


图 2-8 无线节点模块

飞思卡尔（Freescale）公司 MC13224 是第 3 代 ZigBee 解决方案，集成了完整低功耗 2.4GHz 无线电收发器，基于 32 位 ARM7 核的 MCU，用于 IEEE802.15.4 、MAC 和 AES 安全加密的硬件加速器以及 MCU 成套外设，是高密度低元件数 IEEE802.15.4 综合解决方案，能实现点对点连接和完整的 ZigBee 网状网络，因此可广泛应用在住宅区和商业自动化、工业控制、HVAC、卫生保健和消费类电子等产品。

MC13224 支持国际 802.15.4 标准以及 ZigBee、ZigBee PRO 和 ZigBee RF4CE 标准。提供了 104dB 的链路质量、优秀的接收器灵敏度和健壮的抗干扰性，多种供电模式以及一套广泛的外设集——包括 2 个高速 UART、12 位 ADC 和 64 个通用 GPIO，4 个定时器，I2C 等。除了更强 MCU，改进了 RF 输出功率、灵敏度、选择性，且一般会提供一个超越上一代 CC2430 的重要性能改进。除了通过优秀的 RF 性能、选择性和业界标准 ARM7TDMI-S 内核，支持一般低功耗无线通信，还可以配备一个标准网络协议栈（ZigBee、ZigBee RF4CE）来简化开发，使用户更快地获得市场。MC13224 可以用于的应用包括远程控制、

工业控制、HVAC、卫生保健消费型电子、家庭控制、计量和智能能源、楼宇自动化、医疗以及更多领域。

（1）特性：

强大无线前端。

2.4GHz IEEE802.15.4 标准射频收发器。

出色的接收器灵敏度和抗干扰能力。

可编程输出功率为 +4dBm，总体无线连接 104dBm。

极少量的外部元件。

支持运行网状网系统。

-96dBm 接收灵敏度。

250kb/s 数据传输速率。

（2）低功耗：

接收模式	22mA
发送模式 1dBm	29mA
功耗模式 1	3.3mA
功率模式 2	0.8μA
功耗模式 3	0.3μA
宽电源电压范围	2~3.6V

（3）微控制器：

32 位 ARM7TDMI-S 微控制器内核。

128kB 系统可编程闪存。

96K SRAM 及 80K ROM。

硬件调试支持。

（4）外设：

KBI 及 I2C。

4 个 16 位定时器及 PWM。

红外发生电路。

32KHz 的睡眠计时器和定时捕获。

CSMA/CA 硬件支持。

精确的数字接收信号强度指示/LQI 支持。

温度传感器。

两个 8 通道 12 位 ADC。

AES 加密安全协处理器。

两个高速同步串口。

64 个通用 I/O 引脚。

看门狗定时器。

（5）应用：

2.4GHz 的 IEEE802.15.4 标准系统。

RF4CE 遥控控制系统。

HVAC/楼宇自动化。
照明系统。
工业控制和监测。
低功率无线传感网。
消费电子。
健康照顾和医疗保健。

2.3 现代无线传感网主芯片

现代无线传感网主芯片对比见表 2-1。

表 2-1 现代无线传感网主芯片对比表

项 目	CC2430	CC2530	MC13224
引 脚	48	40	99
封 装	QLP48	QFN40	LGA
电 压	2.0～3.6V	2.0～3.6V	2.0～3.6V
大 小	7mm×7mm	6mm×6mm	9.5mm×9.5mm
微控制器	增强型 C8051	增强型 C8051	ARM7TDMI-S
Flash	32/64/128KB	32/64/128/256KB	128KB
RAM	8KB SRAM，4KB Data	8KB	96KB，80KB ROM
段 频	2.4G	2.4G	2.4G
支持标准	ZigBee04/06/SimpliciTI	ZigBee07/PRO/ RF4CE/SimpliciTI	ZigBee07/PRO/RF4CE
软件平台	IAR	IAR	IAR
射频 RF	CC2420	CC2520	MC13224
接收灵敏度	-90dBm	-97dBm	-96dBm（DCD 模式） -100dBm（NCD 模式）
输出功率	0（最小为-3）dBm	4.5（最小-8， 最大 10）dBm	-30～4dBm
自带传感器	温度	温度	温度
功 耗	RX：27mA	RX：24mA	RX：22mA
	TX：25mA	TX：29mA	TX：29mA
低功耗	掉电：0.9μA	掉电：1μA	掉电：0.8μA
	挂起：0.6μA	挂起：0.4μA	挂起：0.3μA
抗干扰	CSMA/CA	CSMA/CA	CSMA/CA
DMA	支持	支持	支持
RSSI/LQI	支持	支持	支持
AES 处理器	有	有	有
I/O	21 个	21 个	64 个
定时/计数器	4（2 个 16 位、2 个 8 位）	4（2 个 16 位、2 个 8 位）	4（16 位）
串 口	2 个	2 个	2 个（2M）
802.15.4 定时器	有	有	有
ADC	8～14 位	7～12 位	12 位
WSN 平台	C51RF-WSN-CC2430	EXPLORERF-CC2530	EXPLORERF-MC13224

2.3.1 ARM 内核 MC13224

飞思卡尔半导体推出一种基于 ZigBee 规范的单芯片平台解决方案，旨在实现业界最低的功耗和最高的性能。MC13224 的设计目标是将电池寿命延长到 20 年，即当前 ZigBee 解决方案的两倍。

飞思卡尔的 MC13224 在 Platform in Package（PiP）解决方案中提供。该解决方案在单一封装中集成了 ZigBee 应用所有必要的组件，从而可减少组件数量并降低系统成本。MC13224 包括一个 32 位微控制器（MCU）、一个完全符合 IEEE802.15.4 标准的射频收发器以及不平衡变压器和射频（RF）匹配组件。所有这些都集成到一个小巧的矩栅阵列（LGA）封装中，几乎可以彻底消除对外部射频组件的需求。该解决方案还支持可以将节点之间的数据速率提高到 2Mb/s 的 TurboLink 技术模式。

飞思卡尔与客户密切合作，共同确定下一代 ZigBee 解决方案应具备的最佳特性。全新设计了 ZigBee Platform in Package，以便在一个高度集成的封装中实现最低功耗和最高性能。MC13224 设计面向需要在 IEEE802.15.4 或 ZigBee 网络中更快地传输音频和数据文件的新型无线设备。

为全球公用事业行业提供先进测量技术的领导者 Itron 公司已选择 ZigBee 标准来在其 OpenWay 高级测量基础设施（AMI）平台上支持家庭能量管理和负载控制应用。

Itron 的 OpenWay AMI 系统产品线经理 Arun Sehgal 表示："通过以经济的价位提供高性能的功能，ZigBee 解决方案（如飞思卡尔的 MC1322x Platform in Package）旨在帮助公用事业机构为大众市场上的个人用户部署先进的能量管理和负载控制功能。这种功能为电力公司提供了新的工具来有效地管理峰值负载，同时可以帮助客户作出明智的选择，使他们可以在家中节约能源和开支。ZigBee 无线通信不仅可以在大众市场上实现这一切，而且它还非常经济有效。"

Schneider Electric 公司电子和软件研究总监 Jean-Pierre Desbenoit 表示："飞思卡尔的 Platform in Package 为其他全球 ZigBee 无线通信平台提供商提高了标准。这个平台很好地说明了开放标准的技术可为 OEM 带来什么——激发生产创新的解决方案的一流厂商之间的积极竞争。我深信，MC13224 平台将推动 ZigBee 技术取得新的成功。"

ZigBee 技术目前主要用于工业、商业和医疗应用，如能量管理和资产跟踪。飞思卡尔专用的 TurboLink 技术模式可以将数据速率提高到 2Mb/s，因此可以提供一个理想的平台来支持各种应用，如语音、无线耳机和压缩音频以及大量数据的传输。对于医疗保健相关的应用，如病人监控系统，TurboLink 技术还支持从身体传感器中实时收集数据。然后这些数据可以通过 ZigBee 网络发送到中心地点进行监控。

MC1322x 器件可以在 IEEE802.15.4 协议和 TurboLink 技术分组之间自动切换，使开发人员可以充分利用高速功能，同时监控 ZigBee 网状网络。这种高速功能可以为新设计和应用创造巨大的商机。

MC13224 平台完全重新设计用于支持电池供电的应用。MC1322x 最适合使用锂离子或镍镉电池，可以支持如硬币大小的电池或使用标准的碱性电池，提供长达 20 年的系统寿命。

MC13224 PiP 解决方案的特性如下：

32 位处理器，能够以 26MHz 的频率运行。

IEEE802. 15. 4 收发信机。

硬件加速器和安全性。

支持超低功率应用的机载降压转换器。

双 12 位模数转换器。

多个串行端口和外围设备。

板上 ROM，包括设备驱动器和完全兼容的 IEEE802. 15. 4 2006MAC。

RAM 和闪存可为对成本敏感的无线应用提供灵活而强大的平台。

所有的射频调谐组件和不平衡变压器都包含在 MC1322x 封装中，运行时只需连接一根天线和晶体。飞思卡尔计划向 MC1322x 系列中增加基于 RAM 和闪存的 PiP 解决方案。

飞思卡尔 BeeKit Wireless Connectivity Toolkit 提供了一种易于使用的配置工具来帮助创建各种网络：从简单的点到点网络到全面的 ZigBee 网状网络。

2. 3. 2 C51 内核 CC2530

ZigBee 新一代 SOC 芯片 CC2530 是真正的片上系统解决方案，支持 IEEE802. 15. 4 标准/ZigBee/ZigBee RF4CE 和能源的应用，拥有庞大的快闪记忆体多达 256 个字节。CC2530 是理想 ZigBee 专业应用，支持新 RemoTI 的 ZigBee RF4CE（这是业界首款符合 ZigBee RF4CE 兼容的协议栈）和更大内存大小将允许芯片无线下载，支持系统编程。此外，CC2530 结合了一个完全集成的、高性能的 RF 收发器与一个 8051 微处理器，8KB 的 RAM，32/64/128/256KB 闪存以及其他强大的支持功能和外设。

CC2530 提供了 101dB 的链路质量、优秀的接收器灵敏度和健壮的抗干扰性，四种供电模式，多种闪存尺寸以及一套广泛的外设集——包括 2 个 USART、12 位 ADC 和 21 个通用 GPIO 以及更多。除了通过优秀的 RF 性能、选择性和业界标准增强 8051MCU 内核，支持一般的低功耗无线通信，CC2530 还可以配备 TI 的一个标准兼容或专有的网络协议栈（RemoTI，Z-Stack 或 SimpliciTI）来简化开发，使用户更快地获得市场。CC2530 可以用于的应用包括远程控制、消费型电子、家庭控制、计量和智能能源、楼宇自动化、医疗以及更多领域。

（1）特性：

强大无线前端。

2. 4GHz IEEE802. 15. 4 标准射频收发器。

出色的接收器灵敏度和抗干扰能力。

可编程输出功率为 +4. 5dBm，总体无线连接 102dBm。

极少量的外部元件。

支持运行网状网系统，只需要一个晶体。

6mm×6mm 的 QFN40 封装。

适合系统配置符合世界范围的无线电频率法规：欧洲电信标准协会 ETSI EN300 328 和 EN 300 440（欧洲），FCC 的 CFR47 第 15 部分（美国）和 ARIB STD-T-66（日本）。

（2）低功耗：

接收模式　　24mA

发送模式 1dBm	29mA
功耗模式 1（4 微秒唤醒）	0.2mA
功率模式 2（睡眠计时器运行）	1μA
功耗模式 3（外部中断）	0.4μA
宽电源电压范围	2～3.6V

（3）微控制器：
高性能和低功耗 8051 微控制器内核。
32/64/128/256/KB 系统可编程闪存。
8KB 的内存保持在所有功率模式。
硬件调试支持。
（4）外设：
强大五通道 DMA。
IEEE802.15.4 标准的 MAC 定时器，通用定时器（1 个 16 位，2 个 8 位）。
红外发生电路。
32KHz 的睡眠计时器和定时捕获。
CSMA/CA 硬件支持。
精确的数字接收信号强度 RSSI 指示/LQI 支持。
电池监视器和温度传感器。
8 通道 12 位 ADC，可配置分辨率。
AES 加密安全协处理器。
两个强大的通用同步串口。
21 个通用 I/O 引脚。
看门狗定时器。
（5）应用：
2.4GHz IEEE802.15.4 标准系统。
RF4CE 遥控控制系统（需要大于 64KB）。
ZigBee 系统/楼宇自动化。
照明系统。
工业控制和监测。
低功率无线传感网。
消费电子。
健康照顾和医疗保健。

2.4 无线传感网可视化监控软件

某科技公司无线传感器监控软件是专门为探索系列 EXPLORERF-MC13224 无线传感网实验平台开发的，是基于 .NET 集成开发平台开发的无线传感网上位机可视化监控软件，如图 2-9 所示。

该无线传感器监控软件提供网络拓扑可视化显示、传感器节点数据可视化显示（如温度、光敏值、信号强度等）、各节点的配置及程序下载、扩展实验的配置。该无线传感器

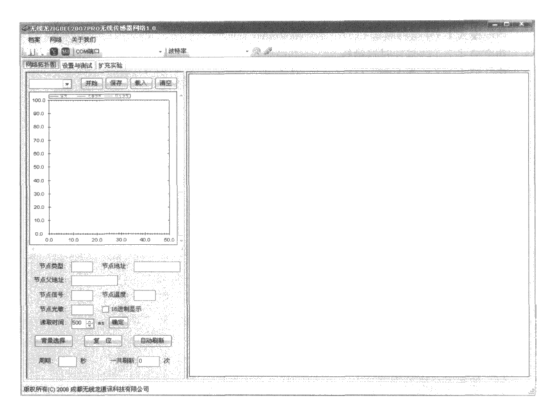


图 2-9 无线网络监控软件界面

监控软件具有如下功能特点：

（1）监测并管理传感器网络。

（2）可视化显示传感器数据。

（3）网络状况监测。

（4）发送命令和激励信号。

（5）节点配置功能。

当无线传感器监控软件接收到数据后，需要对数据进行处理和界面显示。同时对数据和界面进行操作会造成系统阻塞。利用多线程技术，将数据的处理和图形的界面显示分开实现，可以解决系统阻塞问题，它能够可靠地执行并行性任务，并提高了数据处理效率和系统性能，使得界面流畅。界面显示作为主线程，负责维护界面。在程序执行过程中，调用数据处理线程，它们负责各种数据的分析与处理、存储和传送等。

采用模块化设计，使得整个系统层次清晰，可扩展性良好，根据需要进行扩展，具有很大的灵活性。添加新的功能模块，并不需要改变系统的整体框架，并且系统维护简单可靠。

在监控软件的设计中，着重实现了以下 3 个功能模块：

（1）感知数据表格化显示。系统会收到传感器节点采集的一系列环境数据，例如温度、光强、加速度、位置等各种感知数据，利用表格化实时动态地将这些数据显示出来，使研究人员直

观地观察到每个节点的运行状态，从而掌握监控区域小范围内的状态，如图2-10所示。

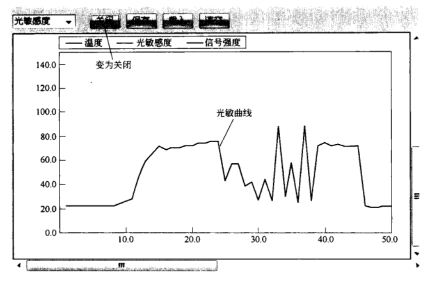


图2-10 曲线显示

（2）网络拓扑结构。实时显示网络中的拓扑结构，同时可以显示节点的路由状态和链路信息，掌握网络运行的整体状态。增加拖动功能，研究人员可以根据自己的需要，在屏幕范围内任意拖动节点位置，方便观察，利于研究，如图2-11所示。

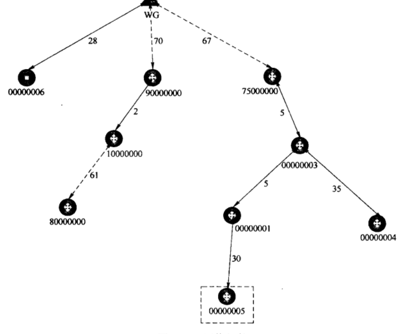


图2-11 网络拓扑

（3）节点管理。控制传感节点数据采集，控制传感节点、监控节点状态等。如图 2-12 所示。

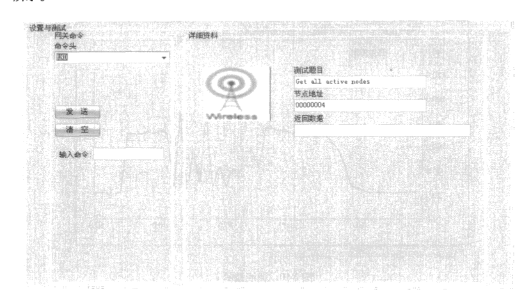


图 2-12　节点管理

监控终端软件流程框架如下：

（1）用户登录，界面初始化；

（2）连接前端服务器控制程序，连接成功后前端服务器向客户端发送数据；

（3）将所有的原始数据信息显示到实时信息输出区；

（4）收到数据包后判断节点类型和传感器板类型；

（5）根据节点类型和传感器板类型建立活动列表，同时将实时数据存入到数据库；

（6）设置定时器，在一定时间段内，如果没有某个节点的数据包到达，说明该节点能耗耗尽或者发生意外情况，将该节点从活动节点列表中删除，但是记录下该节点的活动情况；

（7）在程序界面的左方节点列表区域显示所有活动节点信息；

（8）在感知数据视图、拓扑结构视图和跟踪定位视图中进行动态显示。

2.5　软件开发编译仿真环境

2.5.1　WSN 软件开发环境

IAR Embedded Workbench（简称 EW）的 C/C ++ 交叉编译器和调试器是当今世界最完整和最容易使用的专业嵌入式应用开发工具。EW 对不同的微处理器提供一样直观用户界面。

EW 今天已经支持 35 种以上的 8 位、16 位以及 32 位 ARM 的微处理器结构。

EW 包括嵌入式 C/C ++ 优化编译器、汇编器、连接定位器、库管理员、编辑器、项

目管理器和C-SPY调试器。使用IAR的编译器最优化最紧凑的代码，可节省硬件资源，最大限度地降低产品成本，提高产品竞争力。

EWARM是IAR目前发展很快的产品，EWARM已经支持ARM7/9/10/11XSCALE，并且在同类产品中具有明显价格优势。其编译器可以对一些SOC芯片进行专门的优化，如Atmel、TI、ST、Philips。除了EWARM标准版外，IAR公司还提供EWARM BL（256K）版本，方便了不同层次客户的需求。

IAR System是嵌入式领域唯一能够提供这种解决方案的公司。EW支持35种以上的8位、16位、32位的微处理器结构。

IAR Embedded Workbench集成的编译器主要产品特征如下：

（1）高效PROMable代码。

（2）完全标准C兼容。

（3）内建对应芯片的程序速度和大小优化器。

（4）目标特性扩充。

（5）版本控制和扩展工具支持良好。

（6）便捷的中断处理和模拟。

（7）瓶颈性能分析。

（8）高效浮点支持。

（9）内存模式选择。

（10）工程中相对路径支持。

我们为什么要放弃使用其他各种免费的开发工具，而选择需要支付费用来购买的IAR Systems开发工具？主要包括以下几点原因：

（1）由于IAR公司在微处理器C/C++编译器设计方面的丰富经验，目前没有任何一家公司的产品可以接近IAR公司针对8位、16位、32位处理器生产的30多种不同C/C++编译器的水平。

（2）经过反复实验证明，IAR Systems的C/C++编译器可以生成高效可靠的可执行代码，并且应用程序规模越大，效果明显。与其他的工具开发厂商相比，系统同时使用全局和针对具体芯片的优化技术。连接器提供的全局类型检测和范围检测对于生成目标代码的质量至关重要。

（3）IAR Systems一贯使用精简的优化技术——基于最新技术架构的，针对AVR的IAR Embedded Workbench4.10B版，生成的代码的尺寸比3.20A版缩小了10%，远远小于其他同类编译器生成的代码尺寸。IAR Embedded Workbench生成的可以执行代码可以运行于更小尺寸、更低成本的微处理器之上，从而降低产品的开发成本。

为什么小就意味着完美？因为紧缩的代码，就说明它可以很好地运行在更小、更便宜的芯片上！假设公司要生产10000设备，而每一台因为使用了更小尺寸处理器的设备可以节省2美元，这对公司来说将是一笔很客观的收入。产品的成本对于设计部门来说不是最先考虑的因素也不是开发工具的任务，但是它确是产品或销售经理最感兴趣的内容。

尺寸小不仅仅意味着廉价，它也为各种附加的功能留下了充足的扩展空间。假设客户中途需要为产品设计增加一些新的功能特性，而在这个阶段再去选择另一款芯片是不可行的。这时，IAR Systems提供的高效的编译器加上代码检测服务为公司在最终期限之前完

成任务提供了可能。应该清楚这种情况在以前的工作中会经常遇到。

忽略项目的最终期限，开发者需要依靠一些可靠的开发工具来完成任务。未能按时完成进度会给项目带来不便，而恶性循环将会导致所有进度安排的拖延，后果变得十分严重。IAR Embedded Workbench 被认为是一款稳定可靠的开发工具，它提供连续的工作流，使开发者可以专心于项目的开发，提高开发效率。

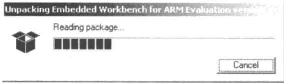
IAR Embedded Workbench 是一套完整的集成开发工具集合，包括从代码编辑器、工程建立到 C/C ++ 编译器、连接器和调试器的各类开发工具。它和各种仿真器、调试器紧密结合，使用户在开发和调试过程中，仅仅使用一种开发环境界面，就可以完成多种微控制器的开发工作。

除上述的几点之外，IAR Embedded Workbench、IAR Systems 还提供了 visual STATE 和 IAR Make App 两套图形开发工具帮助开发者完成应用程序的开发，它可以根据设计自动生成应用程序代码和自动生成驱动程序，使开发者摆脱这些耗时的任务同时保证了代码的质量。

不论客户在哪里，IAR Systems 都可以为其提供完善的技术支持和设计服务。

下面我们就从安装到设置一步一步地学习如何使用 IAR 集成开发环境。

如同 Windows 操作系统其他一般的软件安装一样，单击 EWARM-EV-WEB-520. exe 进行安装，将会看到如图 2-13 所示的界面。



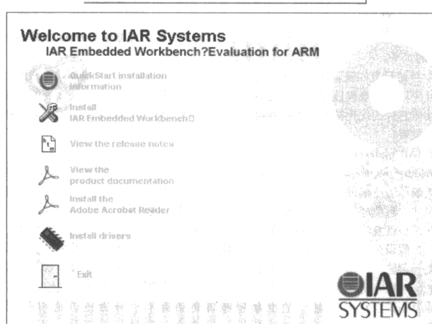
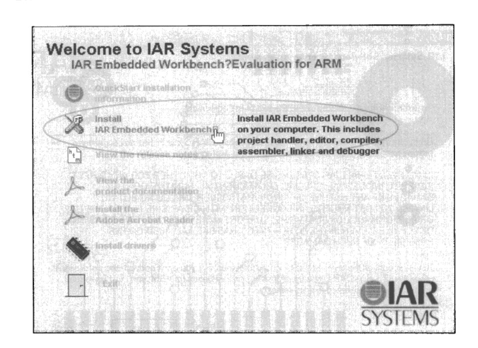


图 2-13　IAR 安装欢迎界面

选择“Install IAR Embedded Workbench”开始安装，如图2-14所示。



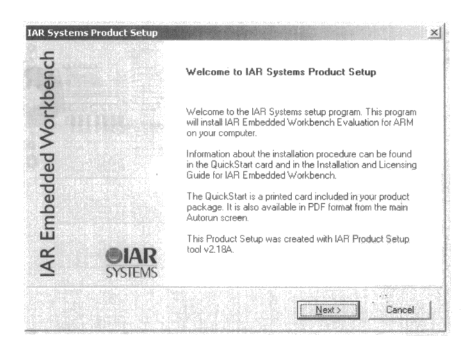


图2-14 IAR开始安装

单击"Next"至下一步，如图 2-15 所示。

IAR Systems Product Setup

IAR Systems Software License Agreement

IAR SYSTEMS

Press the PAGE DOWN key to see the rest of the agreement.

Other use than for evaluation and testing is prohibited. IAR Systems has no obligation to provide support or related services, and gives no warranties.

IN NO EVENT SHALL IAR SYSTEMS BE LIABLE TO THE OTHER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE OR TORT DAMAGES OF ANY NATURE OR KIND WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOST PROFITS, IN CONNECTION WITH OR ARISING OUT OF THE USE OR PERFORMANCE OF SOFTWARE, SUPPORT MATERIALS, OR THE PROVISION OF SERVICES, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Do you accept all the terms of this License Agreement? If you don't accept, the installation is cancelled. To install IAR Embedded Workbench Evaluation for ARM, you must have read, understood, and accepted this agreement.

InstallShield

< Back　Accept　Cancel

IAR Systems Product Setup

Enter User Information

IAR SYSTEMS

Enter your name, the name of your company, and your IAR Embedded Workbench Evaluation for ARM license number.

Name: cyy

Company: wxl

The license number can be found on the CD cover.

License#: 3053-495-666-0782

InstallShield

< Back　Next >　Cancel

IAR Systems Product Setup

Enter License Key

IAR SYSTEMS

The license key can be either your QuickStart key or your permanent key.
If you enter the QuickStart key (found on the CD cover), you have 30 days to try the product out.
If you have received the permanent key via email, you paste it into the License Key textbox.

License #: 3053-495-666-0782

License Key:

VA45TCG5S8AYCXWZ20KE0G02EJYH91RD9O0CZU61PQ7LWCRGVS44S955DYAKFBWT
W20UQ8EISGMS8QK0BWMNVLQK3WVWG8TZLXFHSDYLEMXKTPV2JXDFCDLANDZ3QT
E3MXUSNRPHVC2GZ2KDJOSR54ZRZWZZCVED2BXULUTYSPYWSR2TKNAUD0IYP4SY
#

Read License Key From File

C: Browse...

< Back   Next >   Cancel

IAR Systems Product Setup

Select Destination Folder

IAR SYSTEMS

Setup will install IAR Embedded Workbench Evaluation for ARM in the following folder.

To install in this folder, click Next. To install in a different folder, click Browse and select another folder.

Destination Folder

C:\...\Embedded Workbench 5.0 Evaluation   Browse...

InstallShield

< Back   Next >   Cancel

图 2-15　IAR 安装过程

正确填写相关信息后，单击“Next”至下一步，如图 2-16 所示。

IAR Systems Product Setup

Performing Operations

IAR SYSTEMS

IAR Embedded Workbench Evaluation for ARM Setup is performing the requested operations.

C:\...\arm\examples\Atmel\at91lib\peripherals\rtt\rtt.c

26%

InstallShield

Cancel

IAR Systems Product Setup

IAR Embedded Workbench

Setup Complete

Setup has finished installing IAR Embedded Workbench Evaluation for ARM on your computer.

The release notes are available from the Start menu.

☑ Yes, I want to read the release notes.

☑ Yes, I want to launch IAR Embedded Workbench.

Click Finish to complete Setup.

IAR SYSTEMS

< Back Finish

图 2-16 IAR 安装完成

单击“Finish”来完成安装。

完成安装后，可以从“开始”那里找到刚刚安装的 IAR 软件，如图 2-17 所示。

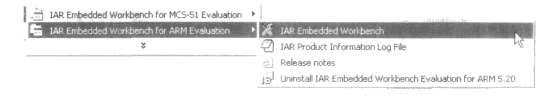


图 2-17 IAR 程序

现在可以通过在桌面的快捷方式或在“开始”按键中选择程序来启动 IAR 软件开发环境。

2.5.2 WSN 仿真驱动

RDI 是 ARM 公司提出的调试接口标准，主要用于 WSN 以 ARM 为内核芯片的 JTAG 仿真。由于各个 IDE 厂商使用的调试接口各自独立，硬件无法进行跨平台的调试。现在众多的 IDE 厂家都逐步采用标准 RDI 作为 ARM 仿真器的调试接口，因此使跨平台的硬件调试成为可能。

MC13224 系列无线传感网开发系统采用 ZigBee 芯片 MC13224 内核是 ARM7，因此为了更方便地开发、调试、仿真，需安装 RDI 驱动。

如同 Windows 操作系统其他一般的软件安装一样，单击 Setup_JLinkARM_V402c. exe 进行安装，将会看到如图 2-18 所示的界面。

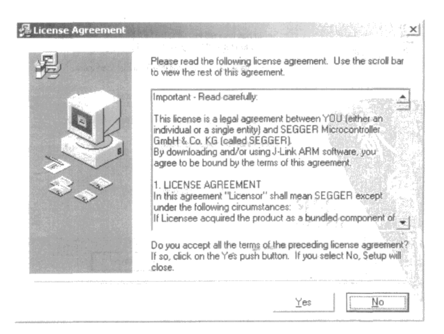
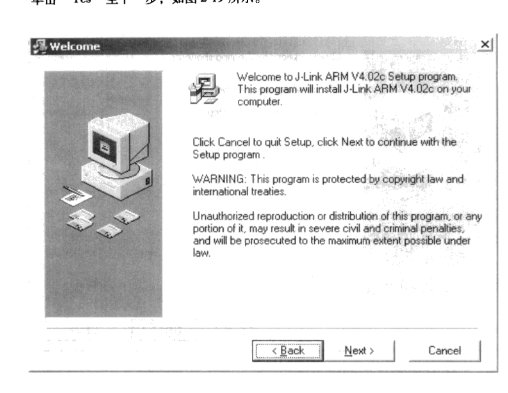
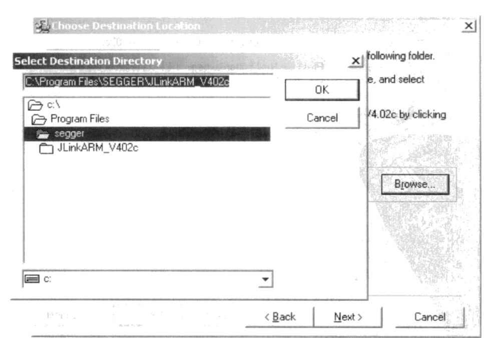


图 2-18 仿真驱动安装

单击“Yes”至下一步，如图 2-19 所示。





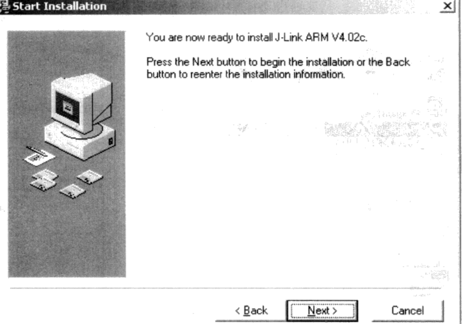
Choose options

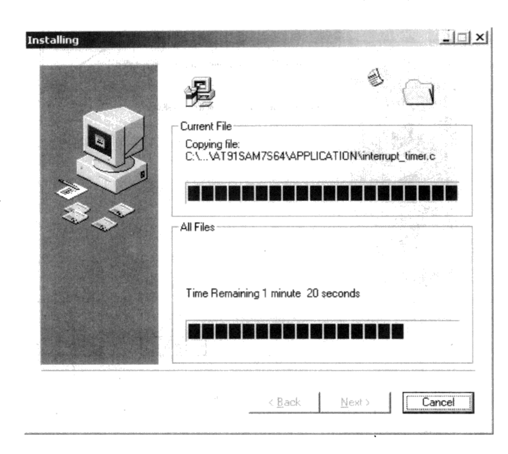
Choose options for creating shortcuts

☑ Create entry in start menu

☐ Add shortcuts to desktop

< Back　Next >　Cancel





SEGGER J-Link DLL Updater V4.02c

The following 3rd-party applications using JLinkARM.dll have been found:

☑ IAR Embedded Workbench Evaluation for ARM 5.20 (DLL V3.86g in "C:\Program Files\IAR Systems\Embedded Workbench 5.0 Evaluation\ARM\bin")

Select All | Select None

Select the ones you would like to replace by this version.
The previous version will be renamed and kept in the same folder, allowing manual "undo".
In case of doubt, do not replace existing DLL(s).
You can always perform this operation at a later time via start menu.

Ok | Cancel

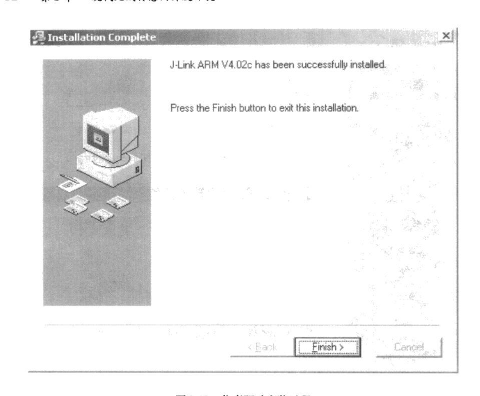


图 2-19　仿真驱动安装过程

单击“Finish”完成安装。

2.6　现代无线传感网络平台使用

现代无线传感器网络平台使用包括软件配置、硬件设置及软硬件综合使用——无线传感网平台仿真调试。

2.6.1　软件集成开发环境配置

了解如何新建一个 IAR 工程及 IAR 相关设置。

(1) 新建工程：打开 IAR 5.20 软件，进入 IAR 界面后，选择菜单“Project/Create New Project”进入新建工程界面，如图 2-20 所示。

在新建工程界面选择，参照图 2-21 选择参数，完成后，点击“OK”保存工程。

如图 2-22 所示，选择保存路径并为工程起好名称后，点“保存”按钮保存工程。应牢记新建工程文件的保存路径。

(2) 添加文件：参照图 2-23 所示方框位置，右击鼠标弹出菜单，选择“Add/Add files”。

添加三个库文件（位于“\ 演示及开发例子程序 \ 基础实验 \ 工程模版 \ Lib”目录下）nit-IAR. s、LLC. a 及 MACPHY. a，如图 2-24 所示。

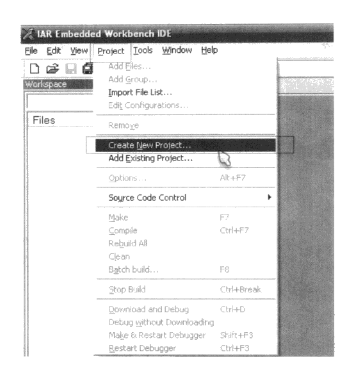


图 2-20 新建工程

Create New Project

Tool chain: ARM

Project templates:

Empty project
asm
C++
C
Externally built executable

Description:

Creates an empty project.

OK Cancel

图 2-21 保存设置

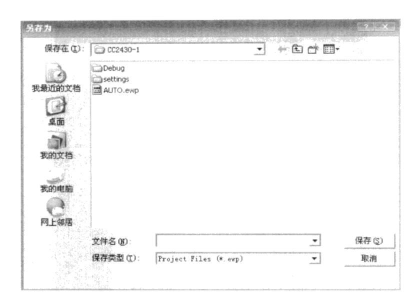


图 2-22　保存

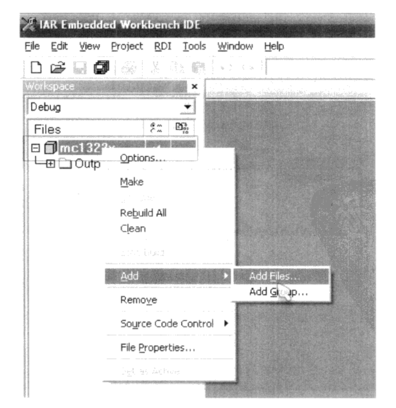
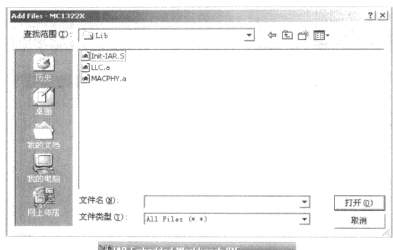


图 2-23　添加



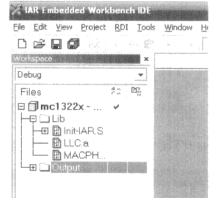


图 2-24 添加库文件

（3）新建程序文件：如图 2-25 所示，点方框中的图标，IAR 弹出新建的文件界面。

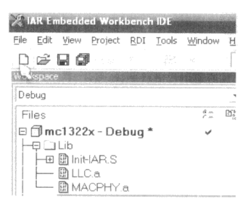


图 2-25 新建程序文件

输入完程序后，点击“🖫”图标，保存文件，如图 2-26 所示。

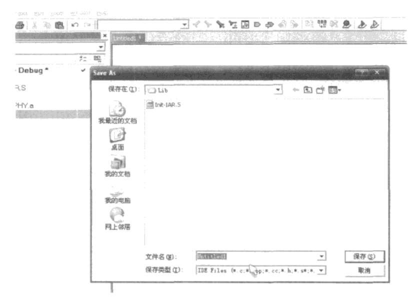


图 2-26　保存工程

完成新建文件后，参照“添加库文件”的方法，加载到工程中。应牢记新建程序文件的保存路径。

（4）设置工程参数：参照图 2-27 所示方框位置，右击鼠标弹出菜单，选择“Options”

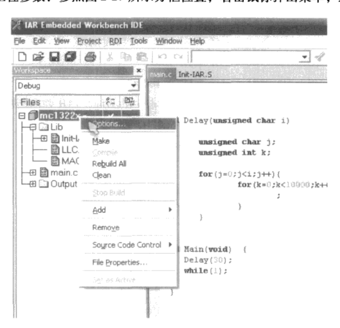


图 2-27　设置

选项，进入参数设置界面。

图 2-28 为参数设置界面。

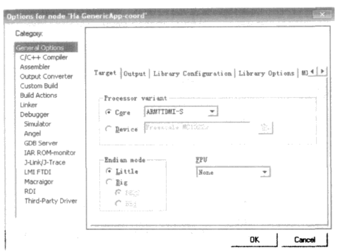


图 2-28 设置界面

在 “General Options” →Library Options 选择参数，如图 2-29 方框中所示。

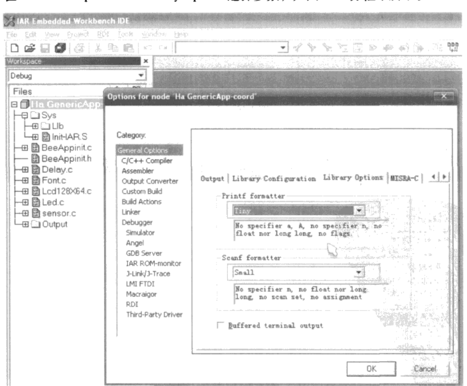


图 2-29 Library Options

在“C/C++Compiler”→Code 选择参数，如图 2-30 方框中所示。

图 2-30 Code

在“Linker”→Config，选择图 2-31 方框中所示选项，在输入框中写入 MC1322x-

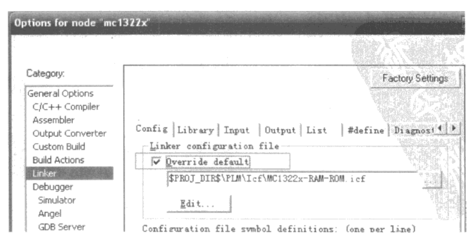


图 2-31 Config

RAM-ROM. icf 文件路径。

在“Linker”→Library，选择图 2-32 方框中所示选项，在红色输入框中写入“_start_vector_”。

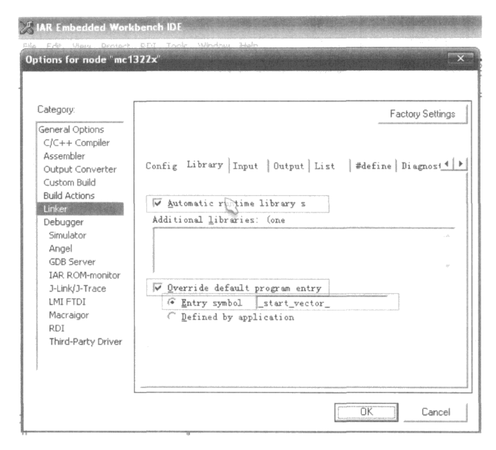


图 2-32 Library

在“Linker”→List，选择图 2-33 方框中所示选项。

在“Debugger”→Setup，选择图 2-34 方框中所示选项，参照图 2-34，输入 FlashMC1322x. mac 文件的路径和 MC1322x. ddf 路径。

在“Debugger”→Debugger，选择图 2-35 方框中所示选项，按“Edit”按钮，设置 Flash 下载相关参数。

在 Flash 下载参数设置界面，按“New”键，新建一个设置，如图 2-36 所示。

参照图 2-37 方框中输入框，输入 FlashMc1322x. out 文件路径和“-eraseall”，设置参数完成后，点“OK”键完成设置。

在“RDI”→RDI，参照图 2-38 输入 JLinkRDI. dll 路径（注：这个文件在 RDI 安装路径下面）。

完成上述设置项后，点“OK”，保存设置参数。

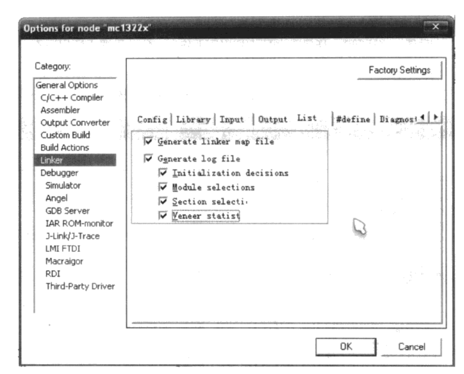


图 2-33　Linker

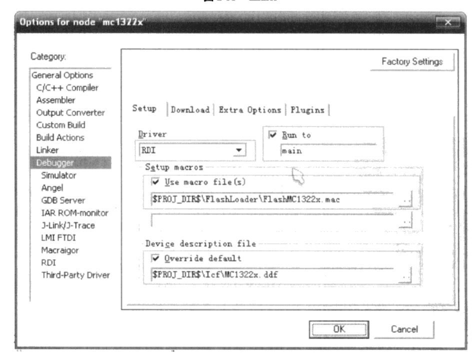


图 2-34　Setup

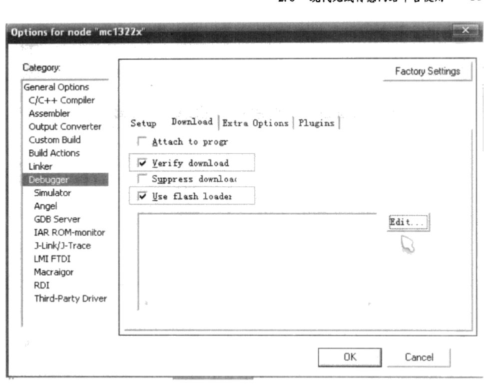


图 2-35　Dowload

Options for node "mc1322x"
Category:
General Options
C/C++ Compiler
Factory Settings
Flash Loader Overview
Range　Offset　Loader Path　Extra Parameters
OK
Cancel
New...
Third-Party Driver
OK
Cancel

图 2-36　新建

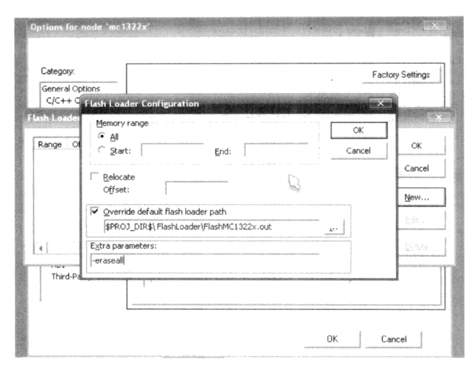


图 2-37　Flash

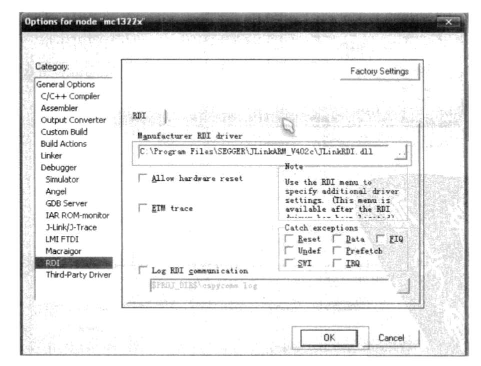


图 2-38　RDI

2.6.2 平台仿真调试

平台仿真调试过程如下：

（1）完成硬件连接及硬件配置。

（2）安装必要软件及驱动。

（3）把例子程序复制至 IAR 安装盘根目录（如 C：\）下。

（4）使用 IAR5.20 打开工程文件。

（5）打开工程文件，如图 2-39 所示。

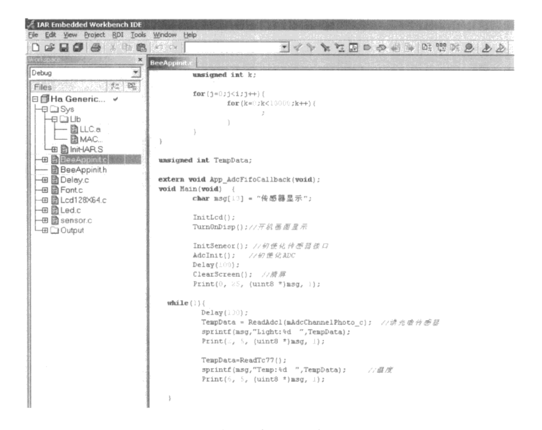


图 2-39 打开工程文件

（6）编译工程，如图 2-40 所示。

点击菜单 Project，选择“Rebuild All”，等待一会儿工程文件编译完成。

（7）把仿真器与网关通过仿真器下载线连接起来，如图 2-41 所示。

（8）确保仿真器与计算机、仿真器与网关液晶底板连接正确，ZigBee 无线模块正确地插在网关底板后，打开网关液晶板上的电源开关。

点击菜单 Project，选择“Download and Debug”，或点击如图 2-42 图标，等待一会儿即完成程序下载，即进行调试状态，如图 2-43、图 2-44 所示。

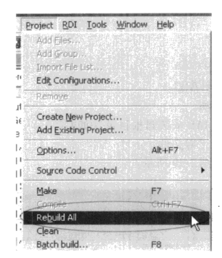


图 2-40 编译

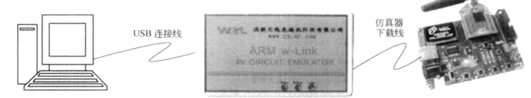


图 2-41 连接

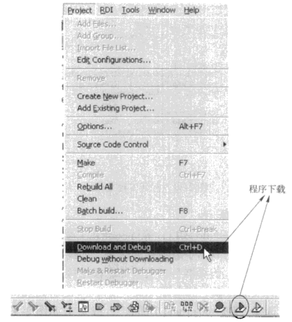


图 2-42 程序下载

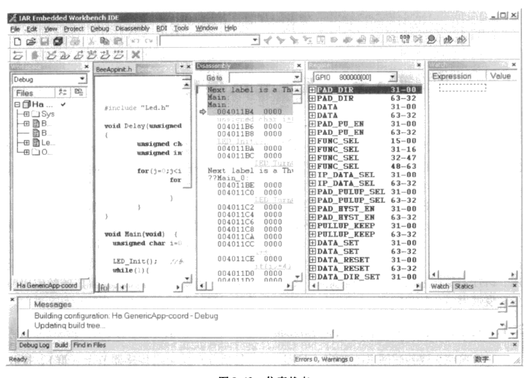


图 2-43 仿真状态

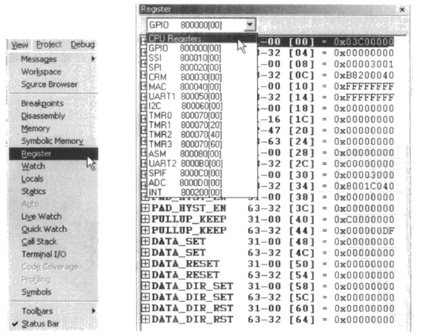


图 2-44 查看各状态及寄存器值

第3章　现代无线传感网技术

无线传感器网络（Wireless Sensor Network，WSN）综合了传感器、嵌入式计算、分布式处理和无线通信等技术，是一种全新的信息获取和处理技术。WSN 由随机分布的集成传感器、数据处理单元和通信模块的微小节点通过自组织的方式构成。它借助于节点中内置的形式多样的传感器，协作地实时监测、感知和采集各种环境或监测对象的信息，对其进行处理，并通过无线和自组多跳的网络方式，将获取到的信息送到终端用户，实现了物理世界、计算机世界和人类社会的有效连通。无线传感器网络因其抗毁性强、监测精度高、覆盖区域大等特点，通常运行在人无法接近的恶劣甚至危险的远程环境中，在军事应用、医疗卫生、远程监控、环境监测、智能家庭网络、抢险救灾等领域有着广阔的应用前景和发展潜力。

3.1　典型无线传感器节点结构和原理

一个典型无线传感网系统架构（见图 1-7）包括分布式无线传感器节点（群）、接收发送器汇聚节点（网关）、数据中心（任务管理）等。

大量传感器节点随机部署在监测区域内部或附近，能够通过自组织方式构成网络。传感器节点监测的数据沿着其他传感器节点逐跳地进行传输，在传输过程中监测数据可能被多个节点处理，经过多跳后路由到汇聚节点，最后通过互联网或卫星到达数据中心。

无线传感器节点通常是一个微型嵌入式系统，它的处理能力、存储能力和通信能力相对较弱，通过携带能量有限的电池供电，如图 3-1 所示。

在不同应用中，传感器节点的组成不尽相同，但一般都由数据采集（传感器模块）、数据处理（处理器模块）、数据传输（无线通信模块）和电源管理这 4 部分组成，如图 3-2 所示。

根据具体应用需求，还可能会有定位系统以确定传感节点的位置，有移动单元使得传感器可以在待监测地域中移动，或具有供电装置以从环境中获得必要的能源。此外，还必须有一些应用相关部分，例如，某些传感器节点有可能在深海或者海底，也有可能出现在化学污染或生物污染的地方，这就需要在传感器节点的设计上采用一些特殊的防护措施。

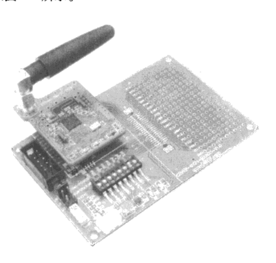


图 3-1　传感器节点

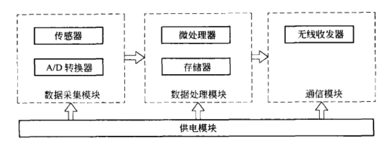


图 3-2 传感器节点体系结构

传感器模块用于感知、获取检测区域内的信息，并将其转换为数字信号，它由传感器和数、模转换模块组成。

处理器模块负责控制和协调节点各部分的工作，存储和处理自身采集的数据以及其他节点发来的数据，它由嵌入式系统构成，包括处理器（如图 3-3 和图 3-4 所示）、存储器等。

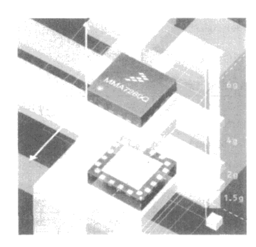


图 3-3 三维加速度传感器

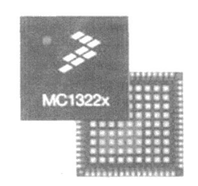


图 3-4 嵌入式处理器

无线通信模块负责与其他传感器节点进行无线通信，交换控制消息和收发采集数据，如图 3-5 所示。



图 3-5 无线芯片

电源管理模块为无线传感器节点提供正常工作所必需的能量，通常采用微型电池。

由于具体的应用背景不同，目前国内外出现了多种无线传感网节点的硬件平台。典型的节点包括 Mica 系列、Sensorial WINS、Toles、μAMPS 系列、XYZnode、Zabranet、无线龙系列等。

实际上各平台的最主要区别是采用了不同的处理器、无线通信协议和与应用相

关的不同的传感器。常用的无线通信协议有 802.11b（Wi-Fi）、802.15.4（ZigBee）、Bluetooth、UWB 和自定义协议，如图 3-6 所示；处理器从 4 位的微控制器到 32 位 ARM 内核的高端处理器都有所应用。还有一类节点是用集成了无线功能的单片机。表 3-1 列出了几种典型无线传感网节点。

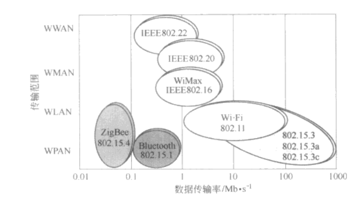


图 3-6 无线通信协议

表 3-1 典型无线传感网节点

节点名称	处理器	无线芯片（技术）	电池类型	发布日期
WeC	AT90S8535（Atmel）	TR1000（RF）	Lithium	1998
Renee	ATmega163（Atmel）	TR1000（RF）	AA	1999
Mica	ATmega128L（Atmel）	TR1000（RF）	AA	2001
Mica2Dot	ATmega128L（Atmel）	CC1000（RF）	Lithium	2002
Mica3	ATmega128L（Atmel）	CC1020（RF）	AA	2003
Toles	MSP430F149（TI）	CC2420（ZigBee）	AA	2004
Platform1	PIC16LF877（Microchip）	Bluetooth&RF	AA	2004
Platform3	ARM7TDMI 核 + Bluetooth 集成（Zeevo）		Battery	2005
Zabranet	MSP430F149（TI）	9Xstream（RF）	Batteries	2004
C51RFWSN1	CC2430（ZigBee）		AA	2006
C51RFWSN 2	MSP430F	CC2520（ZigBee）	AA	2008
ARMRFWSN	GS1010（Wi-Fi）		AA	2008
EXPLORERF	MC13224（ZigBee）		AA	2009

3.1.1 核心微控制器

处理器模块包括主要微控制器及存储器，是传感器网络节点的核心，和其他模块一起完成数据的采集、处理和收发。

微控制器是将微型计算机的主要部分集成在一个芯片上的单芯片微型计算机。微控制器诞生于 20 世纪 70 年代中期，经过 30 多年的发展，其成本越来越低，而性能越来越强大，这使其应用已经无处不在，遍及各个领域。例如电机控制、条码阅读器（扫描器）、

消费类电子、游戏设备、电话、HVAC、楼宇安全与门禁控制、工业控制与自动化、无线传感网和白色家电（洗衣机、微波炉）等。

微控制器，如图3-7所示是中央处理器、存储器、定时（计数）器、中断系统、输入输出接口都集成在一块集成电路芯片上的微型计算机。与应用在个人电脑中的通用型微处理器相比，它更强调自供应（不用外接硬件）和节约成本。它的最大优点是体积小，可放在仪表内部，但存储量小，输入输出接口简单，功能较低。

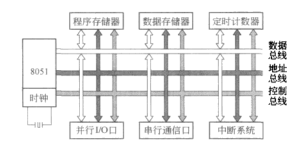


图3-7 C51内核

微控制器可从不同方面进行分类：根据数据总线宽度可分为8位、16位和32位机；根据存储器结构可分为Harvard结构和Von Neumann结构；根据内嵌程序存储器的类别可分为OTP、掩膜、EPROM/EEPROM和闪存Flash；根据指令结构又可分为CISC（Complex Instruction Set Computer）和RISC（Reduced Instruction Set Computer）微控制器。

从微控制器角度看，无线传感网节点基本可以分为两类：一类采用以ARM处理器为代表的高端处理器。该类节点的能量消耗比较大，多数支持DVS（动态电压调节）或DFS（动态频率调节）等节能策略，但是其处理能力也强很多，适合图像等高数据量业务的应用。另一类是以采用8051微控制器为代表的节点。该类节点的处理能力较弱，但是能量消耗功率也很小。在选择处理器时应该根据实际应用考虑系统对处理能力的需要及功耗问题。

3.1.2 无线收发器

传感器节点之间以及传感器节点与汇聚节点（网关）之间都需要通过无线通信方式交互信息，如图3-8所示，无线通信方式可以有多种方式，如红外、声波及射频等。在传感

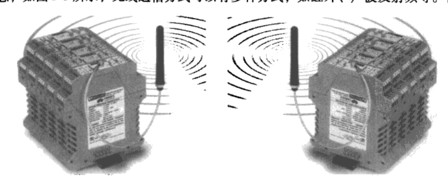


图3-8 无线模块

器节点中，无线通信模块非常重要，因为发送和接收消息所需要的能量是节点总能耗的绝大部分。

无线通信模块主要结构是无线通信芯片，如图3-9所示，无线通信芯片由频率合成器、接收解调器、功率放大器、晶体振荡器和调制器组成，不需外加声表滤波器，使用SPI接口与微控制器通信，配置非常方便。无线通信编码、解码由片内硬件完成，无需用户对数据进行编码、解码，因此使用非常方便。此外其功耗非常低，内建空闲模式与关机模式，易于实现节能。一般工作于315MHz、433MHz、868MHz、915MHz、2.4GHz等ISM（工业、科学和医学）频道。无线通信芯片适用于无线数据通信、无线报警及安全系统、无线开锁、无线监测、工业自动化、无线传感网、RFID、无线抄表、农业监控、家庭自动化和玩具等诸多领域。

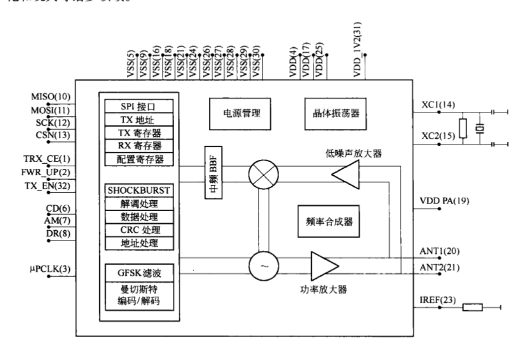


图3-9 无线芯片内部结构

无线通信芯片根据支持通信标准不同分为支持国际通信标准及自定义通信标准。如支持ZigBee无线网络国际通信标准的CC2420、CC2430、CC2530、MC13193、MC13224等，支持自定义通信标准的CC1100、CC2500、NRF905、NRF24L01等。

设计和选择无线通信芯片时，需要考虑三个不同的层：物理层、媒体访问层和网络层。物理层负责在发送端和接收端之间建立物理链路，主要的任务有：为了在有信道噪声及信号干扰的情况下，保持通信质量而使用的信号调制、数据编码；为了有效使用基带及一定程度地减少开发成本，比较好的方法是多个无线模块使用相同的媒介。媒体共享（如时间或者频率）是由媒体访问层（MAC Layer）来实现的。最后网络层负责建立消息传输的路径。

下面介绍基于无线传感器网络平台 EXPLORERF-MC13224 或 DREAMRF-MC13224 的两个无线网络节点实现 MAC 层无线收发通信。

ZigBee 芯片 MC13224 包含一个硬件模块，它提供了低层 MAC 和 PHY 链接控制器，连同运行 ARM 内核软件，实现了基带协议和其他低级别的链接例行控制和连接控制。MACA (802.15.4MAC Accelerator) 组成部分包括顺序列的控制器与定时器、Tx 和 Rx 包缓冲器、DMA 模块、帧校验序列（FCS）发生器、检查和控制寄存器。

作为 802.15.4 协议的一部分，数据包生成和传输，数据包接收和验证，以及能源通道是通过一个信道评估（CCA）的测量。此外，组合或序列活动需要作为协议的一部分，如一个收到的数据包后 ACK 响应。CPU 方便通过 MACA 控制这些活动的收发器和关闭加载功能。一个专用的 DMA 功能来移动 MACA 缓冲区数据和 RAM 数据；不需要 CPU 干预。

MACA 负责建设 TX 数据包（含 FCS），并分解接收包。MACA 还将运行 ACKs 和 Tx-poll 独立序列的 ARM 处理器。在 MACA 处理 TX 期间将构建完整数据包。这包括序言和 SFD（帧首定界符）。在接收期间，调制解调器将承认序言和 SFD，然后将在 MACA 将开始接收数据包的第一个位的帧长度，最后将检查 FCS。

图 3-10 所示为基于 MC13224 的 802.15.4 的 MAC 低层应用系统框图。

基于 MAC 低层应用可以是任何应用，这完全取决于用户，如：MAC 专用应用、ZigBee 网络层应用、其他专利应用。

MAC 低层与应用层之间提供了 3 个接口。

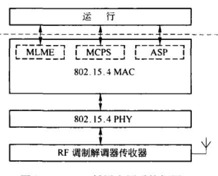


图 3-10　MAC 低层应用系统框图

使用无线传感器网络平台的网关（如图 3-11 所示）建立基于 MAC 无线网络、无线网络节点（如图 3-12 所示）加入 MAC 无线网络后，通过节点上传感器采集数据并上传给网

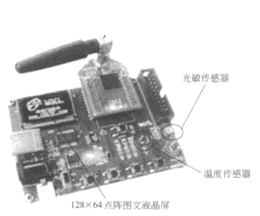
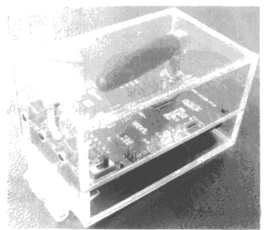


图 3-11　网关


图 3-12　网络节点

关，网关通过串口显示出来。

3.1.2.1 源代码分析

网关程序中无线数据接收处理函数如下：

```
/*************************************************************************
* The App_HandleMcpsInput(mcpsToNwkMessage_t * pMsgIn) function will handle
* messages from the MCPS, e.g. Data Confirm, and Data Indication.
* 无线数据接收处理函数。
*************************************************************************/
unsigned char LED1Value = 0;
static void App_HandleMcpsInput(mcpsToNwkMessage_t * pMsgIn)
{ char msg[30];
  switch(pMsgIn->msgType)
  {
      /* The MCPS-Data confirm is sent by the MAC to the network or application layer when data has been
sent. */
  case gMcpsDataCnf_c:
    if(mcPendingPackets)
      mcPendingPackets--;
    break;
  case gMcpsDataInd_c:
    /* The MCPS-Data indication is sent by the MAC to the network or application layer when data has been re-
ceived. We simply copy the received data to the UART. */
    //接收到无线的数据,通过串口向 PC 机发送.
          if(LED1Value == 0) {
            Led1Off();
            LED1Value = 1;
          }
          else {
            Led1On();
            LED1Value = 0;
          }
    //LCd 显示数据包长度
    sprintf(msg, "RXD Length:%d", pMsgIn->msgData.dataInd.msduLength);
    PrintV(5,3,(uint8 *)msg,1);
    //数据长度
    memset(msg,' ',30);
    sprintf(msg, "RXD Length: %d", pMsgIn->msgData.dataInd.msduLength);
    UartUtil_Tx((uint8_t *)msg,27);//串口发送数据
    //RF 接收的数据
    memset(msg,' ',30);
    UartUtil_Tx(pMsgIn->msgData.dataInd.pMsdu,pMsgIn->msgData.dataInd.msduLength);
```

```
    //串口发送数据
    msg[0] = 10;
    msg[1] = 13;
    UartUtil_ Tx ( (uint8_ t*) msg, 2); //串口发送数据
    break;
  }
}
```

传感器采集数据程序如下：

```
/*********************************************************************
  uint16 ReadAdc1(uint8 channel)
  光敏传感器采集数据
*********************************************************************/
uint16 ReadAdc1(uint8 channel)
{
    uint16 AdcValue;
    AdcFifoStatus_t fifoStatus;
    AdcFifoData_t adcFifoData;
    uint8_t  adcFifoLevel;
        AdcConvCtrl_t adcConvCtrl;
    /* Set conversion control */
    adcConvCtrl.adcTmrOn = TRUE;
    adcConvCtrl.adcSeqIrqEn = FALSE;
    adcConvCtrl.adcChannels = (1 << channel);
    adcConvCtrl.adcTmBtwSamples = mTimeBetweenSamples_c;
    adcConvCtrl.adcSeqMode = gAdcSeqOnTmrEv_c;
    adcConvCtrl.adcRefVoltage = gAdcExtRefVoltage_c;//外部参考 2.5V
    Adc_SetConvCtrl(gAdcPrimary_c,&adcConvCtrl);//配置 ADC
    DelayMs(5);
    Adc_TurnOn();
    do {
        Adc_GetFifoStatus(&fifoStatus,&adcFifoLevel);
    } while(gAdcFifoEmpty_c == fifoStatus);
    Adc_ReadFifoData(&adcFifoData);
    Adc_TurnOff();
    AdcValue = adcFifoData.adcValue;
    return AdcValue;
}
//温度传感器采集数据
uint8 ReadTc77(void)
{
    uint16 temp = 0;
    uint8 i;
```

```
    GpioPinState_t Bitdata;

    Gpio_SetPinData(TC77_SCK,LOW);
    Gpio_SetPinData(TC77_CS,LOW);

    for(i=0; i<16; i++)
    {
        temp << =1;
        Gpio_SetPinData(TC77_SCK,HIGH);
        asm("nop");
        Gpio_GetPinData(TC77_MISO,&Bitdata);
        if(Bitdata)temp++;
        Gpio_SetPinData(TC77_SCK,LOW);
        asm("nop");
    }
    Gpio_SetPinData(TC77_CS,HIGH);
        i=temp>>7;
    return i;
}
```

以网络节点程序中的定时采集数据任务为例，讲解如何在MAC例程中添加定时任务和一般事件。

任务事件处理函数如下：

```
//扫描传感器
void ScanSersor_Task(event_t events)
{
    /* Start the timer; */
    TMR_StartIntervalTimer(mScanSersorTimerID,gScanSersorInterval_c,ScanSersor);//启动定时任务
}
```

添加事件和定时任务如下：

```
static tsTaskID_t mScanSersorTaskID;    //创建定时任务事件ID
#define gScanSersorInterval_c   3000  //3S 定时时间
tmrTimerID_t mScanSersorTimerID = gTmrInvalidTimerID_c;
//在 void MApp_init(void)函数中
mScanSersorTaskID = TS_CreateTask(gTsScanSersorTaskPriority_c,ScanSersor_Task);
//创建任务事件
mScanSersorTimerID = TMR_AllocateTimer();         //创建时钟ID
TMR_EnableTimer(mScanSersorTimerID);              //使能时钟ID
```

定时采集数据任务函数如下：

```
uint8_t ScanSersorValue[100];
//传感器扫描函数
```

```
unsigned int TempData;
void ScanSersor(uint8_t timerId)
{
    ScanSersorValue[0] = '&';
    ScanSersorValue[1] = '2';
    TempData = ReadAdc1(mAdcChannelPhoto_c);  //读光敏传感器
    sprintf((char *)&ScanSersorValue[2],"Light:%d   ",TempData);
    TempData = ReadTc77();
    sprintf((char *)&ScanSersorValue[12],"Temp :%d   ",TempData);     //温度
    App_TransmitData(&ScanSersorValue[0],22);        //RF 发送数据
}
```

激活事件程序如下：

```
TS_SendEvent(mScanSersorTaskID,gAppEvtRxFromUart_c);
```

RF 数据传输函数如下：

```
/*************************************************************************
* The App_TransmitUartData()function will perform(single/multi buffered)
* data transmissions of data received by the UART. Data could also come from
* other sources such as sensors etc. This is completely determined by the
* application. The constant mDefaultValueOfMaxPendingDataPackets_c determine the maximum
* number of packets pending for transmission in the MAC. A global variable
* is incremented each time a data packet is sent to the MCPS,and decremented
* when the corresponding MCPS-Data Confirm message is received. If the counter
* reaches the defined maximum no more data buffers are allocated until the
* counter is decreased below the maximum number of pending packets.
* The function uses the coordinator information gained during the Active Scan,
* and the short address assigned to us by coordinator,for building an MCPS-
* Data Request message. The message is sent to the MCPS service access point
* in the MAC.
*************************************************************************/
uint8_t App_TransmitData(uint8_t * data,uint8_t dataLeng)
{
      /* Use multi buffering for increased TX performance. It does not really
      have any effect at a UART baud rate of 19200bps but serves as an
      example of how the throughput may be improved in a real-world
      application where the data rate is of concern. */
    if((mcPendingPackets < mDefaultValueOfMaxPendingDataPackets_c)&&(mpPacket == NULL))
  {
  /* If the maximum number of pending data buffes is below maximum limit
      and we do not have a data buffer already then allocate one. */
  mpPacket = MSG_AllocType(nwkToMcpsMessage_t);
  }
```

```
if(mpPacket ! =NULL)
{
    mpPacket->msgData.dataReq.pMsdu=data;//送入要发送的数据
    /* Data was available in the UART receive buffer. Now create an
        MCPS-Data Request message containing the UART data. */
    mpPacket->msgType=gMcpsDataReq_c;//数据类型
    /* Create the header using coordinator information gained during
        the scan procedure. Also use the short address we were assigned
        by the coordinator during association. */
    FLib_MemCpy(mpPacket->msgData.dataReq.dstAddr,mCoordInfo.coordAddress,8);//目的地址
    FLib_MemCpy(mpPacket->msgData.dataReq.srcAddr,maMyAddress,8);//来源地址
    FLib_MemCpy(mpPacket->msgData.dataReq.dstPanId,mCoordInfo.coordPanId,2);//目的 PAN ID
    FLib_MemCpy(mpPacket->msgData.dataReq.srcPanId,mCoordInfo.coordPanId,2);//来源 PAN ID
    mpPacket->msgData.dataReq.dstAddrMode=mCoordInfo.coordAddrMode;//目的地址模式
    mpPacket->msgData.dataReq.srcAddrMode=mAddrMode;    //来源地址模式
    mpPacket->msgData.dataReq.msduLength=dataLeng;  //数据长度
    /* Request MAC level acknowledgement of the data packet
      要求 MAC 水平确认,并间接传输的数据包 */
    mpPacket->msgData.dataReq.txOptions=gTxOptsAck_c;
    /* Give the data packet a handle. The handle is
      returned in the MCPS-Data Confirm message.
      供给数据包的句柄。返回的句柄在 MCP 的数据确认消息 */
    mpPacket->msgData.dataReq.msduHandle=mMsduHandle++;
    /* Send the Data Request to the MCPS 请求发送数据 */
    (void)MSG_Send(NWK_MCPS,mpPacket);
    /* Prepare for another data buffer 准备另外数据缓冲 */
    mpPacket=NULL;
    mcPendingPackets++;
    return 0;
    /* Receive another pressed keys */
}
else //发送失败
{
  return 1;

}
}
```

工程文件如图3-13所示。

3.1.2.2 实验演示

打开网关电源，使网关开启MAC网络，如图3-14所示。按下S1按键，液晶显示如图3-15所示。

图 3-13 工程文件



图 3-14 网关液晶显示



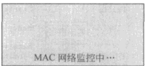


图 3-15 开启网络

网络节点加入 MAC 网络，打开网络节点电源，按下 S1 按键，串口调试助手显示如图 3-16 所示。

网络节点会每间隔 1s，采集一次光敏和温度传感器数据，并发送到网关（协调器）。网关收到节点数据后，会把接收到的数据和数据长度通过串口显示，如图 3-17 所示。

Length 表示数据长度，Light 表示光敏传感器采集数值，Temp 表示温度传感器采集数值。

3.1.3 无线单片机

在无线传感器节点设计常采用两种结构实现方式，一种是采用微控制器 + 无线通信芯片 + 电源 + 传感器结构，另一种采用无线单片机 + 电源 + 传感器结构。这两种结构实现方式最主要的区别在于选择无线通信部分。



图 3-16　串口显示

图 3-17　采集数据显示

在 8051 微控制器内核的片上系统快速发展的同时，短距离无线数据通信使用的无线通信收发集成电路也在高频/CMOS 集成电路技术快速发展的推动下，得到了快速发展。

最新无线收发芯片将全部无线通信需用的调制、解调芯片，高效率高频放大器（低噪声高频放大器）等全部集成在很小的芯片中，外围零件大幅度减少，非常容易接口，低价格微控制器，实现高可靠无线通信。

上述的无线数据通信芯片，虽然已经进行了很大程度上的集成化设计，但是要实现各种实际的无线通信和无线网络，还是必须要有一个微控制器来进行控制，而实行无线网络的各种网络通信协议，无线数据接收、发射等，也需要微控制器来具体处理。

为了适应无线通信和无线网络节点的要求，实现较小的体积、极低的功耗、更低的价格，无线片上系统近年来得到了快速发展，这种无线片上系统将微控制器、存储器、A/D转换器和需要的接口电路和无线数据通信收发芯片全部集成到一个非常小的芯片上。一个独立工作的无线通信和无线网络节点的芯片称为无线单片机。

无线片上系统（无线单片机）出现为开发无线通信和无线网络提供了新的选择，同时也使无线通信和无线网络的设计工作更加简化，更容易开发。

在目前主要有以8051微控制器及ARM微控制器为内核的两种无线单片机，具有代表性的是TI公司CC1010、CC2430、CC2431（如图3-18所示）、CC2530，Freescale公司

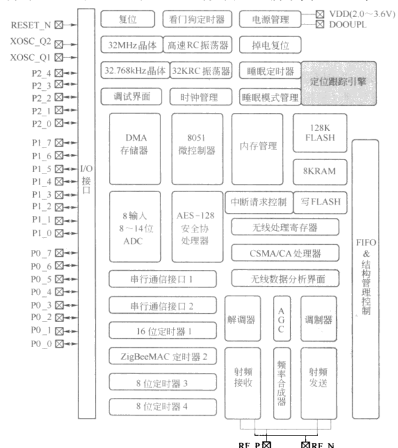


图3-18 CC2431

MC13224 和 Nordic 公司 NRF9E5、NRF24E1。

3.1.4 传感器和执行部件

传感器模块用于感知、获取检测区域内有用信息、数据，并将其转换为数字信号通过无线通信模块传输出去，它由传感器和数、模转换模块组成，如图 3-19 所示。

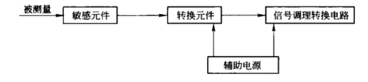


图 3-19 传感器工作原理

3.1.4.1 定义

广义上说，传感器是一种能把物理量或化学量转变成便于利用的电信号的器件。

国际电工委员会（International Electrotechnical Committee，IEC）对传感器的定义为："传感器是测量系统中的一种前置部件，它将输入变量转换成可供测量的信号"。按照 Gopel 等的说法是："传感器是包括承载体和电路连接的敏感元件"，而"传感器系统则是组合有某种信息处理（模拟或数字）能力的传感器"。传感器是传感器系统的一个组成部分，它是被测量信号输入的第一道关口。

国家标准是这样定义"传感器"的，即能感受规定的被测量并按照一定的规律转换成可用输出信号的器件或装置。这一定义包含了以下几方面的意思：（1）传感器是测量装置，能完成检测任务；（2）它的输出量是某一被测量，可能是物理量，也可能是化学量、生物量等；（3）它的输出量是某种物理量，这种量要便于传输、转换、处理、显示等，这种量可以是气、光、电量，但主要是电量（电压、电流、电容、电阻等）；（4）输出输入有对应关系，且应有一定的精确程度。

传感器通常由敏感元件、转换元件和信号调理转换电路三部分组成。

（1）敏感元件：它是直接感受被测量，并输出与被测量成确定关系的某一物理量的元件。

（2）转换元件：敏感元件的输出就是它的输入，它把输入转换成电路参量。

（3）转换电路：电路参数接入基本转换电路（简称转换电路），便可转换成电量输出。传感器只完成被测参数至电量的基本转换，然后输入到测控电路，进行放大、运算、处理等进一步转换，以获得被测值或进行过程控制。

3.1.4.2 分类

传感器种类众多，如图 3-20 所示，可以从不同的方面对传感器进行分类，如它们的转换原理（传感器工作的基本物理或化学效应）、它们的用途、它们的输出信号类型以及制作它们的材料和工艺等。

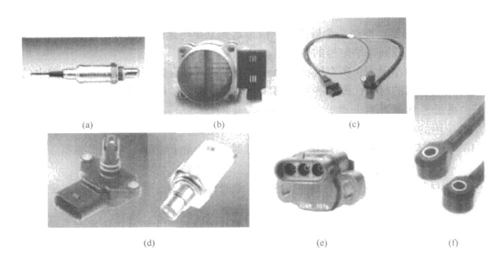


图 3-20 各种传感器
(a) 氧传感器；(b) 负荷传感器；(c) 转速传感器；(d) 温度传感器；
(e) 节气门传感器；(f) 爆震传感器

A 根据传感器转换原理分类

根据转换原理，传感器可分为物理传感器和化学传感器两大类。

物理传感器应用的是物理效应，诸如压电效应，磁致伸缩现象，离化、极化、热电、光电、磁电等效应，被测信号量的微小变化都将转换成电信号。

化学传感器包括那些以化学吸附、电化学反应等现象为因果关系的传感器，被测信号量的微小变化也将转换成电信号。

有些传感器既不能划分为物理类，也不能划分为化学类。大多数传感器是以物理原理为基础运作的。化学传感器技术问题较多，例如可靠性问题、规模生产的可能性、价格问题等，解决了这类难题，化学传感器的应用将会有巨大增长。

B 根据传感器工作原理分类

按照其工作原理，传感器可分为：应变式传感器、电容式传感器、电感式传感器、热电式传感器、光电式传感器、压电式传感器、磁电式传感器、超声波传感器。

C 根据传感器用途分类

按照其用途，传感器可分为：力敏传感器、位置传感器、液面传感器、能耗传感器、速度传感器、热敏传感器、振动传感器、湿敏传感器、磁敏传感器、气敏传感器、真空度传感器、生物传感器、加速度传感器以及射线辐射传感器。

D 根据传感器输出信号分类

以其输出信号为标准可将传感器分为如下几种：

(1) 模拟传感器，即将被测量的非电学量转换成模拟电信号的传感器。

(2) 数字传感器，即将被测量的非电学量转换成数字输出信号（包括直接和间接转换）的传感器。

(3) 膺数字传感器，即将被测量的信号量转换成频率信号或短周期信号的输出（包

括直接或间接转换）的传感器。

（4）开关传感器，即当一个被测量的信号达到某个特定的阈值时，传感器相应地输出一个设定的低电平或高电平信号的传感器。

在外界因素的作用下，所有材料都会做出相应的、具有特征性的反应。它们中的那些对外界作用最敏感的材料，即那些具有功能特性的材料，被用来制作传感器的敏感元件。

E 根据传感器材料分类

从所应用的材料观点出发可将传感器分成下列几类：

（1）按照其所用材料的类别分为金属传感器、聚合物传感器、陶瓷传感器、混合物传感器。

（2）按材料的物理性质分为导体传感器、绝缘体传感器、半导体传感器、磁性材料传感器。

（3）按材料的晶体结构分为单晶传感器、多晶传感器、非晶材料传感器。

与采用新材料紧密相关的传感器开发工作，可以归纳为下述三个方向：

（1）在已知的材料中探索新的现象、效应和反应，然后使它们能在传感器技术中得到实际使用。

（2）探索新的材料，应用那些已知的现象、效应和反应来改进传感器技术。

（3）在研究新型材料的基础上探索新现象、新效应和反应，并在传感器技术中加以具体实施。

现代传感器制造业的进展取决于用于传感器技术的新材料和敏感元件的开发强度。传感器开发的基本趋势是和半导体以及介质材料的应用密切关联的。

F 根据传感器的制造工艺分类

按照其制造工艺，可以将传感器区分为：集成传感器、薄膜传感器、厚膜传感器、陶瓷传感器。

集成传感器是用标准的生产硅基半导体集成电路的工艺技术制造的。通常还将用于初步处理被测信号的部分电路也集成在同一芯片上。

薄膜传感器则是通过沉积在介质衬底（基板）上的相应敏感材料的薄膜形成的。使用混合工艺时，同样可将部分电路制造在此基板上。

厚膜传感器是利用相应材料的浆料，涂覆在陶瓷基片上制成的，基片通常由 Al_2O_3 制成，然后进行热处理，使厚膜成形。

陶瓷传感器采用标准的陶瓷工艺或其某种变种工艺（溶胶-凝胶等）生产。

3.1.4.3 传感器基本特性

传感器的特性是指传感器的输入量和输出量之间的对应关系。通常把传感器的特性分为静态特性和动态特性两种。

静态特性是指输入不随时间而变化的特性，它表示传感器在被测量各个值处于稳定状态下输入输出的关系。

动态特性是指输入随时间而变化的特性，它表示传感器对随时间变化的输入量的响应特性。

一般来说，传感器的输入和输出关系可用微分方程来描述。理论上，将微分方程中的

一阶及以上的微分项取为零时，即可得到静态特性。因此传感器的静特性是其动特性的一个特例。

传感器除了描述输入与输出量之间的关系特性外，还有与使用条件、使用环境、使用要求等有关的特性。

A 传感器的静特性

传感器的输入—输出关系为输入（外部影响，包括冲振、电磁场、线性、滞后、重复性、灵敏度、误差因素）—传感器—输出（外部影响，包括温度、供电、各种干扰稳定性、温漂、稳定性（零漂）、分辨力、误差因素）。

人们总希望传感器的输入与输出成唯一的对应关系，而且最好呈线性关系。但一般情况下，输入输出不会完全符合所要求的线性关系，因传感器本身存在着迟滞、蠕变、摩擦等各种因素，并且受外界条件的各种影响。

传感器静态特性的主要指标有：线性度、灵敏度、重复性、迟滞、分辨率、漂移、稳定性等。

B 传感器的动特性

动特性是指传感器对随时间变化的输入量的响应特性。

很多传感器要在动态条件下检测，被测量可能以各种形式随时间变化。只要输入量是时间的函数，则其输出量也将是时间的函数，其间关系要用动特性来说明。设计传感器时要根据其动态性能要求与使用条件选择合理的方案和确定合适的参数；使用传感器时要根据其动态特性与使用条件确定合适的使用方法，同时对给定条件下的传感器动态误差做出估计。总之，动特性是传感器性能的一个重要方面，对其进行研究与分析十分必要。总的来说，传感器的动特性取决于传感器本身，另一方面也与被测量的形式有关。

（1）规律性的：1）周期性的（正弦周期输入、复杂周期输入）；2）非周期性的（阶跃输入、线性输入、其他瞬变输入）。

（2）随机性的：1）平稳的（多态历经过程、非多态历经过程）；2）非平稳的随机过程。

在研究动态特性时，通常只能根据“规律性”的输入来考虑传感器的响应。复杂周期输入信号可以分解为各种谐波，所以可用正弦周期输入信号来代替。其他瞬变输入不及阶跃输入来得严峻，可用阶跃输入代表。因此，“标准”输入只有三种，即正弦周期输入、阶跃输入和线性输入，而经常使用的是前两种。

3.1.5 通信频率范围和天线

日常生活中，我们经常能够看到各式各样的天线。对于一个无线系统来说，能够正确地发送和接收信息是最基本的要求。天线作为无线通信中不可缺少的一部分，其基本功能就是接收和发送无线电波。发射时，把高频电流转换为电磁波，如图3-21所示；接收时，把电磁波转换为高频电流。那么这么多的电波在空气中是如何传播的，我们又是

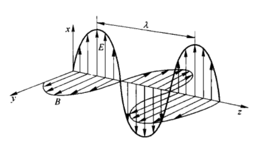


图3-21 沿 z 轴传播的电磁波在某一时刻的波的图像

如何区分哪些是我们需要的电磁波呢？

频谱是我们区别各种电波的一个重要依据，如表 3-2 所示，无线通信的频谱在 RF（Radio Frequency）这一段包括了我们常见的调频收音机、各种手机、无线电话、无线卫星电视等。由于从几十兆到几千兆的频谱上，集中了各种不同的无线应用，而且这些无线电传播都使用同一个通信媒介——空气，所以为了保证各种无线通信之间不相互干扰，就需要对无线频道的使用进行必要的管理。

表 3-2 无线电波波段的划分

波段名称		波长范围	频段名称	频率范围	主要用途
超长波		>1000m	VLF 甚低频	<30kHz	水下通信
长 波		1000 ~ 10000m	LF 低频	300 ~ 30kHz	电 报
中 波		200 ~ 1000m	MF 中频	1500 ~ 300kHz	调幅无线电广播
短 波		50 ~ 200m	IF 中高频	6000 ~ 1500kHz	电报、业余通信、调幅无线电广播
		10 ~ 50m	HF 高频	30 ~ 6MHz	电报、业余通信、调幅无线电广播
超短波	米波	1 ~ 10m	VHF 甚高频	300 ~ 30MHz	电视、导航、业余通信、调幅无线电广播
	分米波	10 ~ 100cm	UHF 特高频	3000 ~ 300MHz	电视、导航、雷达等
微 波	厘米波	1 ~ 10cm	SHF 超高频	30 ~ 3GHz	电视、导航、雷达、卫星通信等
	毫米波	1 ~ 10mm	EHF 极高频	300 ~ 30GHz	雷达、通信、遥感、射电天文等
	亚毫米波	<1mm		>300GHz	雷达、通信、遥感、射电天文等

各国的无线电管理机构负责管理 RF 频道的使用。在美国，这个管理机构是美国联邦通讯委员会（FCC）；在欧洲，是欧洲电信标准化协会（ETSI）；在我国，是中国无线电管理委员会。频道管理最基本的规则是无线发送器的使用需要获得许可。

各国的无线管理部门也规定了某些频带不需许可就可以使用，以满足不同的需要。这些频带通常包括 ISM（Industrial、Scientific and Medical——工业、医疗、科学）频带。各国的无线电管理不尽相同。在美国，FCC 管理无线电频谱的分配。可用的免许可证的频带包括：27MHz、260 ~ 470MHz、902 ~ 928MHz 和最常用的 2.4GHz 频带。其中 260 ~ 470MHz 频带对数据传送的类型有所限制，而其他频带则没有这样的限制。ISM 频道在欧洲所分配到的频率为 433MHz、868MHz 和 2.4GHz。我国目前可以使用的 ISM 频率是：433MHz 和 2.4GHz。

除了 ISM 频带以外，在我国，整个低于 135kHz，在北美、南美和日本，低于 400kHz，也都是可以使用的免费频段。各国对无线频谱资源的管理，不仅规定了相关的 ISM 开放频道的频率，同时也严格规定了在这些频率上所使用的发射功率，在实际使用这些频率时，需要查阅各国无线频谱管理机构的不同的具体技术要求。

我国的无线电管理要求的具体技术参数可查阅信息产业部发布的《微功率（短距离）无线电设备管理暂行规定》。

无线传感器网络国际标准 IEEE802.15.4（ZigBee）工作在工业科学医疗（ISM）

频段，定义了两个工作频段，即2.4GHz频段和868/915MHz频段。在IEEE802.15.4中，总共分配了27个具有3种速率的信道：在2.4GHz频段有16个速率为250kb/s的信道，在915MHz频段有10个40kb/s的信道，在868MHz频段有1个20kb/s的信道。其中2.4G是全球通用的ISM频段，915是北美的ISM频段，868是欧洲的ISM频段。

这些信道的中心频率按表3-3所示定义（k为信道数）。

表3-3 信道的中心频率 (MHz)

信道编号	中心频率	信道间隔	频率上限	频率下限
$K=0$	868.3		868.6	868.0
$K=1, 2, 3, \cdots, 10$	$906+2(k-1)$	2	928.0	902.0
$K=11, 12, 13, \cdots, 26$	$2401+5(K-11)$	5	2483.5	2400.0

一个IEEE802.15.4可以根据ISM频段、可用性、拥挤状况和数据速率在27个信道中选择一个工作信道，如图3-22所示。从能量和成本效率来看，不同的数据速率能为不同的应用提供较好的选择。例如，对于有些计算机外围设备与互动式玩具，可能需要250kb/s速率，而对于其他许多应用，如各种传感器、智能标记和家用电器等，20kb/s这样的低速率就能满足要求。

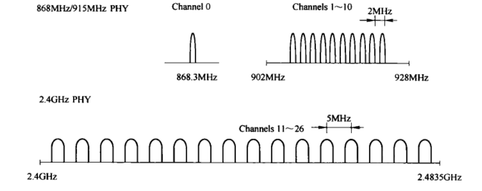


图3-22 ZigBee信道

不同的数据传输率适用于不同的场合。例如，868/915MHz频段物理层的低速率换取了较好的灵敏度和较大的覆盖面积，从而减少了覆盖给定物理区域所需的节点数。2.4GHz频段物理层的较高速率适用于较高的数据吞吐量、低延时或低作业周期的场合。

打开无线传感器网络平台EXPLORERF-MC13224或DREAMRF-MC13224配套提供的任意一个ZigBee实验工程文件，打开ZigBee协议栈配置文件ApplicationConf.h，如图3-23所示。找到如下源代码：

```
/*
    The default channel list defines which channels to scan when forming or joining a
    network. Default = 0x02000000 = channel 25. The channel list is a bitmap, where each
    bit describes a channel (for example bit 12 corresponds to channel 12). Any combination
    of channels can be included. ZigBee supports channels 11-26.
    The default channel list may also be set over-the-air using the Startup Attribute Set
    Cluster, or ZDP Mgmt_NWK_Update_req.

    3 2    2    2    1    1    0    0    0
    1 8    4    0    6    2    8    4    0
    0000 0000 0000 0000 0000 1000 0000 0000 = 0x00000800 = channel 11
    0000 0100 0000 0000 0000 0000 0000 0000 = 0x04000000 = channel 26
    0000 0010 0000 0000 0000 0000 0000 0000 = 0x02000000 = channel 25 (default)
    0000 0111 1111 1111 1111 1000 0000 0000 = 0x07fff800 = all channels 11-26
    0000 0000 1000 0000 0001 0000 0000 0000 = 0x00801000 = channels 23 and 12
    Default: 0x02000000
 */
#ifndef mDefaultValueOfChannel_c
    #define mDefaultValueOfChannel_c          0x00000800
#endif
```

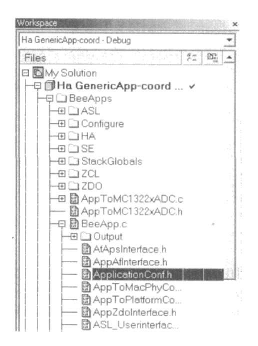


图 3-23 ZigBee 配置文件

由 mDefaultValueOfChannel_ c 来定义 ZigBee 无线传感器网络无线通信信道，本例中

mDefaultValueOfChannel_c 为 0x00000800，即第 11 信道，第 11 信道为 2.405GHz。

为了实现工业、家庭和楼宇的自动化控制，将人类从有线的环境中解放出来，以取代线缆为目标，用于无线个人区域网（WPAN，Wireless Personal Area Network）范围的短距离无线通信技术标准得到了迅速的发展，典型技术标准有蓝牙（Bluetooth）、ZigBee、无线 USB（WirelessUSB）、无线局域网 Wi-Fi（IEEE802.11b/g）等。在人们享受方便快捷的时候，这些技术的电磁兼容问题日益凸显。由于这些技术均选择了 2.4GHz（2.4 ~ 2.483GHz）ISM 频段，再加上无绳电话和微波炉等干扰源，就使得该频段日益拥挤。

2.4GHz 频段日益受到重视，原因主要有三：首先它是一个全球性的频段，开发的产品具有全球通用性；其次，它整体的频宽胜于其他 ISM 频段，这就提高了整体数据传输速率，允许系统共存；第三就是尺寸，2.4GHz 无线电和天线的体积相当小，产品体积也更小。虽然每一种技术标准都进行了必要的设计来减小干扰的影响，但是为了能让各种设备正常运行，对它们之间的干扰、共存分析显然是非常重要的。

ZigBee 技术的抗干扰特性主要是指抗同频干扰，即来自共用相同频段的其他技术的干扰。对于同频干扰的抵御能力是极为重要的，因为它直接影响到设备的性能。ZigBee 在 2.4GHz 频段内具备强抗干扰能力就意味着能够可靠地与 Wi-Fi、蓝牙、WirelessUSB 以及家用的无绳电话和微波炉共存。

IEEE802.15.4 标准中提供了很多机制来保证 ZigBee 在 2.4GHz 频段和其他无线技术标准的共存能力。

IEEE802.15.4 物理层在碰撞避免机制（CSMA/CA）中提供空闲信道评估（CCA，Clear Channel Assessment）的能力，即如果信道被其他设备占用，允许传输退出而不必考虑采用的通信协议。

ZigBee 个人区域网（PAN）中的协调器首先要扫描所有的信道，然后再确认并加入一个合适的 PAN，而不是自己去创建一个新 PAN，这样就减少了同频段 PAN 的数量，降低了潜在的干扰。如果干扰源出现在重叠的信道上，协调器上层的软件要应用信道算法选择一个新的信道。

可以对比 IEEE802.11b 和 IEEE802.15.4 信道算法，如图 3-24 所示，有 4 个 IEEE802.15.4 信道（$n = 15, 16, 21, 22$）落在 3 个 IEEE802.11b 信道的频带间距上，这些间距上的能量不为零，但是会比信道内的能量低，将这些信道作为 IEEE802.15.4 网络工作信道可以将系统间干扰降至最小。

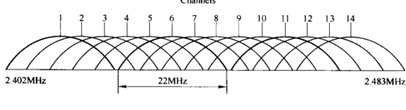


图 3-24 IEEE802.11b 信道

在网络初始化或者响应中断时，ZigBee 设备都会先扫描一系列被列入信道表参数中的信道，以便进行动态信道选择。在有 IEEE802.11b 网络活跃工作的环境中建立一个

IEEE802.15.4 网络，可以按照上述空闲信道来设置信道表参数，以便加强网络的共存性能。

前面介绍 ZigBee 无线信道通过 mDefaultValueOfChannel_c 来定义，在 ZigBee 无线传感器网络建立网络前已经初始化信道，那么 ZigBee 无线传感器网络如何动态选择信道呢?

由 mDefaultValueOfChannel_c 及 gFullChannelList_c 这两个参数来建立动态 ZigBee 信道。如果要把 ZigBee 信道设置在第 11 个及第 12 个信道上动态选择，则 mDefaultValueOfChannel_c 设置为 0x00800800，gFullChannelList_ c 设置为 0x00800800。

```
/*
    The default channel list defines which channels to scan when forming or joining a
    network. Default = 0x02000000 = channel 25. The channel list is a bitmap, where each
    bit describes a channel(for example bit 12 corresponds to channel 12). Any combination
    of channels can be included. ZigBee supports channels 11-26.
    The default channel list may also be set over-the-air using the Startup Attribute Set
    Cluster, or ZDP Mgmt_NWK_Update_req.
    3 2    2    2    1    1    0    0    0
    1 8    4    0    6    2    8    4    0
    0000 0000 0000 0000 0000 1000 0000 0000 = 0x00000800 = channel 11
    0000 0100 0000 0000 0000 0000 0000 0000 = 0x04000000 = channel 26
    0000 0010 0000 0000 0000 0000 0000 0000 = 0x02000000 = channel 25(default)
    0000 0111 1111 1111 1111 1000 0000 0000 = 0x07fff800 = all channels 11-26
    0000 0000 1000 0000 0000 1000 0000 0000 = 0x00800800 = channels 23 and 11
    Default: 0x02000000
*/
#ifndef mDefaultValueOfChannel_c
    #define mDefaultValueOfChannel_c          0x00100000
#endif
/*
    The full channel list defines which channels to scan when forming or joining a network if the
    preferred(mDefaultValueOfChannel_c) didn't work. The channel list is a bitmap, where each bit
    describes a channel(for example bit 12 corresponds to channel 12). Any combination of channels
    can be included. ZigBee supports channels 11-26.
    Set to 0x00000000 to indicate no full channel list should be used(will continued to use
    preferred channel list).
    3 2    2    2    1    1    0    0    0
    1 8    4    0    6    2    8    4    0
    0000 0111 1111 1111 1111 1000 0000 0000 = 0x07fff800 = all channels 11-26
    0000 0000 1000 0000 0000 1000 0000 0000 = 0x00800800 = channels 23 and 11
    Default: 0x00000000(better for demos and lab work)
    ZigBee Default: 0x07fff800(all channels)
*/
#ifndef gFullChannelList_c
    #define gFullChannelList_c          0
#endif
```

天线作为无线通信不可缺少的一部分，如图 3-25 所示，其是一种能量转换器，它的作用是将发射机输出的高频震荡信号转换为电磁波向空中辐射，另一方面，把从空中接受到的电磁波转变成高频震荡信号传输给接收机。

我们来看看天线辐射与波瓣示意图，如图 3-26 所示，其中中间圆体代表天线振子，半透明椭圆体代表辐射波瓣。我们可以看到，在典型的单极天线工作时，辐射的电磁波形状类似于一个苹果，天线振子四周的电磁波平均分布，没有方向性。这是最简单的垂直天线的辐射情况。

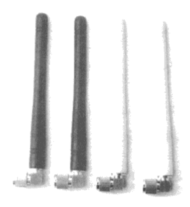


图 3-25 天线

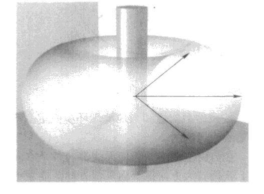


图 3-26 天线辐射与波瓣

天线应用于广播和电视、点对点无线电通信、雷达和太空探索等系统。天线通常在空气和外层空间中工作，也可以在水下运行，甚至在某些频率下工作于土壤和岩石之中。

从物理学上讲，天线是一个或多个导体的组合，由它可因施加的交变电压和相关联交变电流而产生辐射的电磁场，或者可以将它放置在电磁场中，由于场的感应而在天线内部产生交变电流并在其终端产生交变电压。

基于特定三维（通常指水平或垂直）平面，可以把天线分为全向天线和定向天线两大基本类型。

（1）全向天线（在平面中均匀辐射）。全向天线，如图 3-27 所示，即在水平方向图上表现为 360°都均匀辐射，也就是平常所说的无方向性，在垂直方向图上表现为有一定宽度的波束，一般情况下波瓣宽度越小，增益越大。全向天线在移动通信系统中一般应用于郊县大区制的站型，覆盖范围大。

（2）定向天线（又称指向天线，在某方向辐射较多）。如图 3-28 所示，定向天线在水平方向图上表现为一定角度范围辐射，也就是平常所说的有方向性，在垂直方向图上表现为有一定宽度的波束，同全向天线一样，波瓣宽度越小，增益越大。定向天线在移动通信系统中一般应用于城区小区制的站型，覆盖范围小，用户密度大，频率利用率高。

根据组网的要求建立不同类型的基站，而不同类型的基站可根据需要选择不同类型的天线。选择的依据就是上述技术参数。比如全向站就是采用了各个水平方向增益基本相同的全向型天线，而定向站就是采用了水平方向增益有明显变化的定向型天线。一般在市区选择水平波束宽度 B 为 65°的天线，在郊区可选择水平波束宽度 B 为 65°、90°或 120°的天

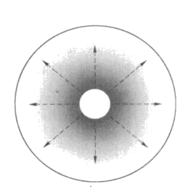


图 3-27 全向天线

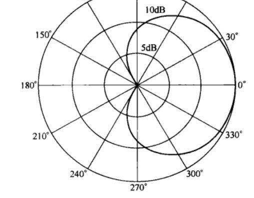


图 3-28 定向天线

线（按照站型配置和当地地理环境而定），而在乡村选择能够实现大范围覆盖的全向天线则是最为经济的。

在自由空间内，任何天线都向各个方向辐射能量，但是特定的架构会使天线在某个方向上获得较大方向性，而其他方向的能量辐射则可以忽略。

通过增加附加导体棒或线圈（称为单元）并改变其长度、间距和方位（或者改变天线波束方向），可以制造出拥有既定特性的天线，如八木天线。“天线阵列”或“天线阵”是指相当数量的有源天线共用源或负载来产生定向的天线辐射方向图。天线的空间关系通常也会影响其方向性。“有源单元”是指此天线单元的能量输出由该单元内部的能量源所决定（而不是仅由通过电路的信号能量）或者该单元能量输出的能量源由信号输入所控制。“天线引入线”是在信号源和有源天线之间传输信号能量的传导装置（如传输线或馈线）。它由有源天线延伸出来直达源。“天线馈电”则是指有源天线和放大器之间的元件。

根据生产工艺及开关不同，天线可分为陶瓷天线、贴片天线、PCB 天线、杆状天线、鞭状天线、板状天线、扇面天线等。

根据工作频段，天线可分为微波天线、短波天线、中波天线、长波天线等。

影响天线性能的临界参数有很多，通常在天线设计过程中可以进行调整，如谐振频率、阻抗、增益、孔径或辐射方向图、极化、效率和带宽等。另外，发射天线还有最大额定功率，而接收天线则有噪声抑制参数。

（1）谐振频率。“谐振频率”和“电谐振”与天线的电长度相关。电长度通常是电线物理长度乘以自由空间中波传输速度与电线中速度之比。天线的电长度通常由波长来表示。天线一般在某一频率调谐，并在此谐振频率为中心的一段频带上有效，但其他天线参数（尤其是辐射方向图和阻抗）随频率而变，所以天线的谐振频率可能仅与这些更重要参数的中心频率相近。

天线可以在与目标波长成分数关系的长度所对应的频率下谐振。一些天线设计有多个谐振频率，另一些则在很宽的频带上相对有效。最常见的宽带天线是对数周期天线，但它的增益相对于窄带天线则要小很多。

（2）增益。天线设计中，“增益”指天线最强辐射方向的天线辐射方向图强度与参考天线的强度之比取对数。如果参考天线是全向天线，增益的单位为 dBi。比如，偶极子天线的增益为 2.14dBi。偶极子天线也常用作参考天线（这是由于完美全向参考天线无法制造），这种情况下天线的增益以 dBd 为单位。

天线增益是无源现象，天线并不增加激励，而是仅仅重新分配而使在某方向上比全向天线辐射更多的能量。如果天线在一些方向上增益为正，由于天线的能量守恒，它在其他方向上的增益则为负。因此，天线所能达到的增益要在天线的覆盖范围和它的增益之间达到平衡。比如，航天器上碟形天线的增益很大，但覆盖范围却很窄，所以它必须精确地指向地球；而广播发射天线由于需要向各个方向辐射，它的增益就很小。

碟形天线的增益与孔径（反射区）、天线反射面表面精度以及发射、接收的频率成正比。通常来讲，孔径越大增益越大，频率越高增益也越大，但在较高频率下，表面精度的误差会导致增益的极大降低。

“孔径”和“辐射方向图”与增益紧密相关。孔径是指在最高增益方向上的“波束”截面形状，是二维的（有时孔径表示为近似于该截面的圆的半径或该波束圆锥所成的角）。辐射方向图则是表示增益的三维图，但通常只考虑辐射方向图的水平和垂直二维截面。高增益天线辐射方向图常伴有“副瓣”。副瓣是指增益中除主瓣（增益最高“波束”）外的波束。副瓣在如雷达等系统需要判定信号方向的时候，会影响天线质量。由于功率分配，副瓣还会使主瓣增益降低。

当两段振子叠加后，波瓣形状变得扁了一些，辐射的能量更集中于水平方向，这就形成了在水平方向上的增益，提高了天线的“效率”，现在市售的玻璃钢基地天线大多采用这种结构，也有很多朋友根据这个原理自制高增益天线。当然，要使天线产生增益并非只有这一种方法。

（3）带宽。天线的带宽是指它有效工作的频率范围，通常以其谐振频率为中心。一般全向天线的工作带宽能达到工作频率范围的 3% ~5%，定向天线的工作带宽能达到工作频率的 5% ~10%。天线带宽可以通过以下多种技术增大，如使用较粗的金属线、加粗天线对称振子导体有效横截面、尖端变细的天线元件、多天线集成单一部件。小型天线通常使用方便，但在带宽、尺寸和效率上有着不可避免的限制。

（4）阻抗。“阻抗”类似于光学中的折射率。电波穿行于天线系统不同部分（电台、馈线、天线、自由空间）会遇到阻抗差异。在每个接口处，取决于阻抗匹配。电波的部分能量会反射回源，在馈线上形成一定的驻波。此时电波最大能量与最小能量比值可以测出，称为驻波比（SWR）。驻波比为 1∶1 是理想情况。1.5∶1 的驻波比在能耗较为关键的低能应用上被视为临界值。而高达 6∶1 的驻波比也可出现在相应的设备中。极小化各处接口的阻抗差（阻抗匹配）将减小驻波比并极大化天线系统各部分之间的能量传输。

天线的复阻抗涉及该天线工作时的电长度。通过调节馈线的阻抗，即将馈线当做阻抗变换器，天线的阻抗可以和馈线和电台相匹配。更为常见的是使用天线调谐器、巴伦、阻抗变换器、包含电容和电感的匹配网络，或者如伽马匹配的匹配段。

（5）辐射方向图。辐射方向图是天线发射或接受相对场强度的图形描述。由于天线向三维空间辐射，需要数个图形来描述。如果天线辐射相对某轴对称（如双极子天线、螺旋天线和某些抛物面天线），则只需一张方向图。

不同的天线供应商和使用者对于方向图有着不同的标准和制图格式。

3.1.6 典型无线传感器节点设计

传感器节点是无线传感网的基本组成单位。它由传感器模块、处理器模块、无线通信模块和能量供应模块四个部分组成。由于传感器节点通常是一个微型的嵌入式系统，它的处理能力、存储能力和通信能力都相对较弱，并通过携带能量有限的电池供电。下面依据传感器节点的这些特点，介绍一种用于环境温、湿度监测，并以无线单片机 CC2430 为核心的无线传感网节点。

3.1.6.1 CC2430 简介

CC2430 芯片是 TI 公司提供给全球的首款支持 ZigBee 协议的 SoC 解决方案。它沿用了 CC2420 芯片的架构，在单个芯片上整合了 ZigBee 射频（RF）前端、内存和微控制器。CC2430 拥有 1 个 8 位 8051MCU，8KB 的 RAM，32KB、64KB 或 128KB 的 Flash，还包含模拟数字转换器、几个定时器、AES128 协处理器、看门狗定时器、32kHz 晶振的休眠模式定时器、上电复位电路、掉电检测电路以及 21 个可编程 I/O 引脚。

CC2430 芯片采用 0.18μm CMOS 工艺生产，工作时的电流损耗为 27mA；在接收和发射模式下，电流损耗分别低于 27mA 或 25mA。CC2430 的休眠模式和转换到主动模式的超短时间的特性，特别适合那些要求电池寿命非常长的应用。

CC2430 芯片的主要特点有：32MHz 单指令周期低功耗的 8051 微控制器核；集成兼容 IEEE802.15.4 标准 2.4GHz 频段的 RF 无线电收发机；8KB 的 SRAM，其中 4KB 可在所有功耗模式下保持数据；兼容 RoHS 的 7mm×7mm QLP 封装；4 种可编程功耗模式；可编程的看门狗定时器；上电复位功能；支持硬件调试功能；优良的无线接收灵敏度和强大的抗干扰性；在休眠模式时仅 0.9μA 的流耗，外部中断或 RTC 能唤醒系统；在待机模式时少于 0.6μA 的流耗，外部中断能唤醒系统；硬件支持 CSMA/CA 功能；较宽的电压范围（2.0～3.6V）；数字化的 RSSI/LQI 支持和强大的 DMA 功能；具有电池监测和温度感测功能；集成了 14 位模数转换的 ADC；集成 AES 安全协处理器；带有两个强大的、支持几组协议的 USART 以及 1 个符合 IEEE802.15.4 规范的 MAC 计时器，1 个常规的 16 位计时器和两个 8 位计时器。

3.1.6.2 节点硬件设计

无线传感网的节点通常由传感器模块、处理器模块、无线通信模块和电源模块构成。处理器模块和无线通信模块采用 CC2430 芯片，大大简化了射频电路的设计。传感器模块采用集成温湿度传感器 SHT10。电源模块采用 3V 纽扣电池。节点的硬件原理框图如图 3-29 所示。

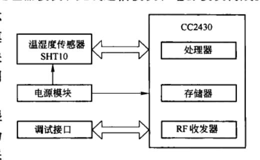


图 3-29 节点的硬件原理图

SHT10 用于采集周围环境中的温度和湿度，其工作电压为 2.4～5.5V，测湿精度为 ±4.5% RH，25℃时测温精度为 ±0.5℃。采用 SMD 贴片封装，与处理器的通信电路如图

3-30 所示。SHT10 采用两条串行线与处理器进行数据通信。SCK 数据线负责处理器和 SHT10 的通信同步；DATA 三态门用于数据的读取。DATA 在 SCK 时钟下降沿之后改变状态，并仅在 SCK 时钟上升沿有效。数据传输期间，在 SCK 时钟高电平时，DATA 必须保持稳定。为避免信号冲突，微处理器应驱动 DATA 在低电平。需要一个 10kΩ 的外部上拉电阻将信号提拉至高电平。本设计中 CC2430 的引脚 P1.0 用于 SCK，P1.1 用于 DATA。

3.1.6.3 节点软件设计

节点的软件分为数据采集、电池能量检测和无线通信这三个分别设计的模块。各个模块的流程图如图 3-31 所示。

A 温湿度数据采集模块

温湿度传感器 SHT10 采用类似但不兼容 I2C 总线的方式和处理器通信。数据通过 DATA 线直接读取，控制流程如图 3-31 所示。首先用一组启动传输时序进行数据传输的初始化，然后发送一组测量命令（'00000101'表示相对湿度，'00000011'表示摄氏温度），释放 DATA 线，等 SHT10 下拉 DATA 至低电平，表示测量结束，同时接收数据。

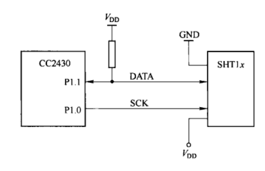


图 3-30 通信电路

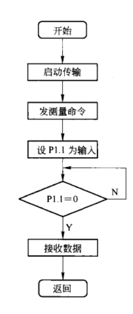


图 3-31 流程图

其中产生启动传输时序的程序片段如下：

```
……
P1_1 = 1;
P1_0 = 1;
wait(1);//等待 1ms
P1_1 = 0;
wait(1);
P1_0 = 0;
wait(1);
P1_0 = 1;
wait(1);
P1_1 = 1;
wait(1);
```

```
P1_0 = 0;
……
```

测量温度后，通过 $T = d1 + d2 \times SOT$ 计算出温度。

测量湿度后，再根据当前的温度，通过 $RH = (T℃ - 25) \times (t1 + t2 \times SORH) + c1 + c2 \times SORH + c3 \times SORH2$，计算出相对湿度。其中常量 $d1$、$d2$、$t1$、$t2$、$c1$、$c2$ 和 $c3$ 由 SHT1x 数据手册提供。

B 电源能量检测模块

无线传感网节点通常采用电池供电，电池的能量检测是重要环节。CC2430 的 ADC 模块不仅可以采样 P0 端口引脚上的输入电压，还可以采样 AVDD_SoC 引脚上的 1/3 电压。这个功能通常用于实现电池的能量检测，即检测当前的电源电压是否在 CC2430 所能工作电压范围 2.0～3.6V 内。完成一次 AD 转换的控制流程是：首先设置 AVDD_SoC 引脚上电压的 1/3 为采样输入，然后启动 AD 转换，等待 AD 转换结束，寄存器 ADCH、ADCL 中的数据即为参考电压的相对数值。

由于是对电池能量的检测，可以采用 CC2430 内部提供的 1.25V 电压作为参考电压。用这个参考电压采样 AVDD_SoC 引脚上的 1/3 电压，从而得出当前的电源电压值。选用 8 位的采样精度，则寄存器 ADCCON3 应配置为 0x0F。设置完寄存器后，ADC 立即启动一次 AD 转化，寄存器 ADCCON1 的 EOC 位用于指示当前的转化是否结束。当 EOC 位变为 1 时，证明当前的转换完成，转换后的数值被存放在寄存器 ADCH 中。ADCH 中的数值被读取后，EOC 位自动恢复为 0。根据取出的数值计算得到当前 AVDD_SoC 上引脚的电压。通过连续采样 10 次进行均值滤波，用这个平均值与用户设定的最低有效工作电压 2.4V 相比，可判断出当前电压是否正常。

其中由 DATA［0…9］的均值 Average 计算实际电压的代码如下：

```
……
Voltage = ((Average * 15) > >9);//Voltage 为实际电压的 10 倍
……
```

C 无线通信模块

无线传感网通信的基础是节点之间的点对点通信。现以两个节点之间的通信为例，介绍点对点通信的过程和实现方法。首先，定义一种比 IEEE802.15.4 规范所定义的 MAC 协议层数据帧简单的 MAC 层数据帧的格式：

1	1	1	1～122	2
目标地址 (DA)	源地址 (SA)	标志位 (Flags)	有效负载 (payload)	帧校验 (FCS)

其中目标地址和源地址分别用 1 个字节表示。本例中只有两个节点互相通信，分别将两个节点的地址设为 0 和 1。标志位 Flags 占 1 个字节，用于表示当前数据帧类型。当数据帧中 Flags 字节最高位为 1 时，表示该帧是数据序列中的一帧；第 3 位为 1 时，表示该帧是超时重传的数据帧；第 2 位为 1 时表示该帧是接收到数据帧后答复帧；第 1 位为 1 时，表示目标节点在收到该数据帧后要答复。帧校验 FCS 由 2 个字节表示，是 MAC 层协议数

据单元 MPDU 的校验。如果 CC2430 的 RF 寄存器 MDMCTRL0L. AUTOCRC 控制位设为 1，FCS 将由硬件自动实现，负责必须由软件用多项式 $x^{16}+x^{12}+x^{5}+1$ 进行 CRC 生成和校验。

由于 IEEE802. 15. 4 规范中定义了物理服务数据单元（PSDU）的最大长度为 127 字节，而其中的 5 字节已经被使用，因此有效负载 payload 字节长度在 1 ~ 122 之间。如果需要传送的数据长度超过 122 字节，则发送时这个数据应该被拆分成若干数据帧，以满足最大长度的限制。目标节点则必须能够将接收到的数据帧整合成完整的数据。

IEEE802. 15. 4 规定了 RF 物理层工作频段为 2. 4GHz，共有 16 个频道。每个频道实际工作频率和频道序号的关系式为：$F_c = 2405 + 5 \times (k - 11)$ MHz，$k = 11, 12, \cdots, 26$。两个节点 RF 必须工作在相同的频道上才能够互相收发数据。完成一次数据发送程序的流程图如图 3-32 所示。

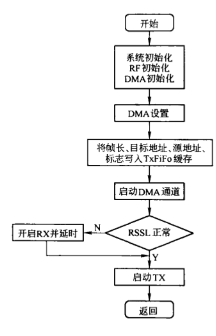


图 3-32 流程图

系统初始化主要是将系统的工作频率设为 32MHz 的晶振频率，这样 RF 才能正常工作。RF 初始化时，先设置通信频率，再通过设置 RFPWR. RREG_RADIO_PD 位为 1 给 RF 供电。RF 初始化的过程还包括执行下面的代码来开启 RX，清空 RX、TX 的 FiFo 缓冲区以及校准 Radio。

```
SRXON;
SFLUSHTX;
SFLUSHRX;
SFLUSHRX;
STXCALN;
ISSTART;
```

DMA 的初始化阶段要为 TX 分配 1 个空闲的 DMA 通道。首先要为通道 0 和通道 1 ~ 4 分别设置好通道描述数据结构的存放地址，并将首地址分别写入 DMA0CFGH：DMA0CFGL 和 DMA1CFGH：DMA1CFGL，再为这个分配好的 DMA 通道设置其描述数据结构。该数据结构如下：

```
    typedef struct {
  BYTE SRCADDRH;//源地址
  BYTE SRCADDRL;
  BYTE DESTADDRH;//目的地址
  BYTE DESTADDRL;
  BYTE VLEN    :3;
  BYTE LENH    :5;
  BYTE LENL    :8;
```

```
    BYTE WORDSIZE :1;
    BYTE TMODE   :2;
    BYTE TRIG   :5;
    BYTE SRCINC   :2;
    BYTE DESTINC   :2;
    BYTE IRQMASK   :1;
    BYTE M8   :1;
    BYTE PRIORITY   :2;
} DMA_DESC;
```

当设置为TX准备的DMA通道时，需将数据的源地址SRCADDRH：SRCADDRL设为所要发送数据的起始地址，目标地址DESTADDRH：DESTADDRL设为寄存器RFD的地址0xDFD9。然后在LENH：LENL中设置所要发送数据的长度，并将VLEN设为0。将WORDSIZE位设为0，表示DMA数据按字节进行传输（设为1表示按字传输）。DMA的数据传送模式按照一次触发传输的数据量可分成四种，由TMODE设置选择。本例中采用Block模式，即一次DMA触发可进行一个完整数据块的传输。CC2430定义的DMA触发信号有31种之多，由TRIG位设置。将TRIG设置为0，表示采用无触发模式，这样DMA在每次接收到DMAREQ信号后才启动一次数据传输。

SRCINC和DESTINC分别用于设置数据源地址和目标地址的变化方式，可设为不变、增1、增2或减1。由于采用按字节的Block模式向Radio发送数据，因此数据源地址选择增1变化，而数据目标地址则一直为寄存器RFD地址0xDFD9，故设为不变。IRQMASK位用于设置是否在DMA数据传输完后发中断信号。本例中设为0，即禁止DMA中断。M8是按字节传输时的数据宽度，设为0表示8位传输，为1时表示只传输字节的低7位。本例中设为0。PRIORITY用于优先级设置，本例中设为2，即中等优先级。

DMA描述设置好后，通过设置寄存器DMAARM和RMREQ位来准备相应DMA通道以及启动这个通道上数据块的传输。在启动DMA数据传输之前，将当前数据帧的长度、目标节点地址、源节点地址、标志字节通过直接写寄存器RFD的方式写入TXFIFO。这样在启动DMA传输后，完整的数据帧将被传输至TXFIFO。通过给CSP发送指令ISTXONCCA启动TX传输。这就完成了一帧数据的发送。

数据接收的过程同样需要设置系统工作频率为32MHz，且应确保RX工作在TX相同的频道上，并设置DMA通道。其中DMA的数据源为寄存器RFD，并将DMA触发信号设为RADIO，即Radio接收到数据时触发DMA。数据接收的程序流程如图3-33所示。

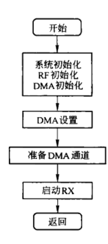


图3-33 数据接收的程序流程

本节在总结归纳对芯片CC2430已有研究成果的基础上，阐述了基于CC2430的无线传感网节点的设计和实现，并详细介绍了两个节点之间点对点通信的实现。在实验中，节点能够采集环境的温、湿度和节点的电池电压，并将采集的数据在节点中传播。本节的研究为进一步的上层通信协议设计提供了基础，具有一定的研究意义。

3.2 无线传感器节点间通信基本技术

无线传感网之间的节点是如何通信的呢？一个节点如何通过无线信号把数据传输至另一个传感器节点？无线传感网采用的即是无线数据通信技术。

数据通信是通信技术和计算机技术相结合而产生的一种新的通信方式。要在两地间传输信息必须有传输信道，根据传输媒体的不同，数据通信有有线数据通信与无线数据通信之分。但它们都是通过传输信道将数据终端与计算机、数据终端与数据终端联结起来，而使不同地点的数据终端实现软、硬件和信息资源的共享。

在没有文字的远古时代，人们是怎样传递信息的呢？那时除了刻一些简单的符号外，结绳记事是很重要的一个办法。如果是大事情，就打个大大的结；如果是小事情，就打小的结。不同数量的结也代表不同的意思。

我国是世界上最早建立有组织的传递信息系统的国家之一。早在三千多年前的商代，信息传递就已见诸记载。乘马传递曰驿，驿传是早期有组织的通信方式。

数据通信的发展有如下几个阶段。

第一阶段：以语言为主，通过人力、马力、烽火等原始手段传递信息，如图 3-34 所示。

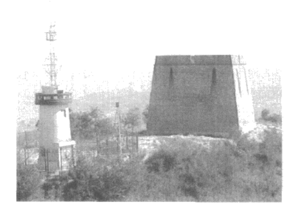


图 3-34 烽火台及无线基站

第二阶段：文字、邮政。（增加了信息传播的手段）

第三阶段：印刷。（扩大信息传播范围）

第四阶段：电报、电话、广播。（进入电器时代）

第五阶段：信息时代，除语言信息外，还有数据、图像、文本等。

3.2.1 数据包

数据通信是依照一定的通信协议，利用数据传输技术在两个终端之间传递数据信息的一种通信方式和通信业务。它可实现计算机和计算机、计算机和终端以及终端与终端之间的数据信息传递。是继电报、电话业务之后的第三种最大的通信业务。

在数据通信中每次传输的数据量是有多有少的，由于发射机及接收机的功能、处理速

度等影响，发射机及接收机不可能一次把所要传输的数据发送出去或接收下来，因此为了规范数据通信传输，需要把传输的数据分成一定数量而且大小相同的包装传输。这样的数据包装称为数据包，如图 3-35 所示。

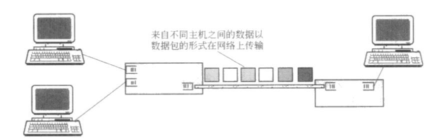


图 3-35 数据包传输

可以用一个形象一些的例子对数据包的概念加以说明：在邮局邮寄产品时，虽然产品本身带有自己的包装盒，但是在邮寄时候只用产品原包装盒来包装显然是不行的。必须把内装产品的包装盒放到一个邮局指定的专用纸箱里，这样才能够邮寄。这里产品包装盒相当于数据包，里面放着的产品相当于可用的数据，而专用纸箱就相当于帧，且一个帧中只有一个数据包。

"包"听起来非常抽象，那么是不是不可见的呢？通过一定技术手段，是可以感知到数据包的存在的。比如在 Windows 系统中，把鼠标移动到任务栏右下角的网卡图标上（网卡需要接好双绞线、连入网络）双击，就可以看到"发送：× ×包，收到：× ×包"的显示框，如图 3-36 所示。

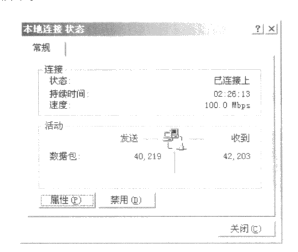


图 3-36 互联网数据包

通过数据包捕获软件，也可以将数据包捕获并加以分析，如图 3-37 所示。用数据包捕获软件捕获到的数据包的界面图中可以很清楚地看到捕获到的数据包的 MAC 地址、IP

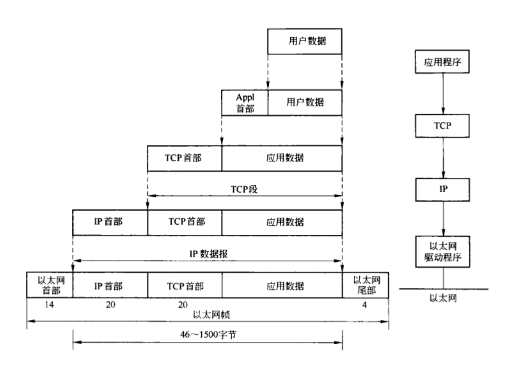


图 3-37 TCP/IP 数据包

地址、协议类型端口号等细节。通过分析这些数据，管理员就可以知道网络中到底有什么样的数据包在活动了。

数据包结构非常复杂，在这里以 ZigBee 网络层的数据包为例来了解它的关键构成，这对于理解数据包是非常重要的。

ZigBee 网络协议数据单元（NPDU）即网络层数据包结构，如图 3-38 所示。

字节	2	2	2	1	1	0/8	0/8	0/1	变长	变长
	帧控制	目的地址	源地址	广播半径域	广播序列号	IEEE 目的地址	IEEE 源地址	多点传送控制	源路由帧	帧的有效载荷
网络层帧报头										网络层的有效载荷

图 3-38 ZigBee 网络层数据包格式

ZigBee 网络协议数据包基本组成部分包括：网络层帧报头，包含帧控制、地址和序列信息；网络层帧的可变长有效载荷，包含帧类型所指定的信息。

图 3-38 表示的是 ZigBee 网络层的通用帧结构，不是所有的帧都包含地址和序列域，但网络层的帧的报头域，还是按照固定的顺序出现，如图 3-39 所示。

有 ZigBee 网络协议中，定义了两种类型的网络层帧，它们分别是数据帧和网络层命令帧。下面来逐个介绍数据包结构中的组成部分。

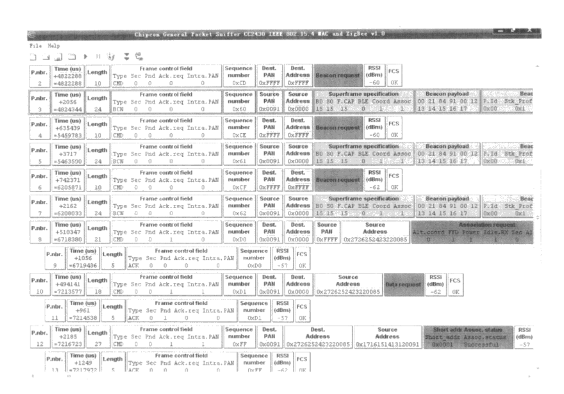


图 3-39 ZigBee 数据包

（1）帧控制域。帧控制域格式如图 3-40 所示，为 16b（位或比特）。可以看到帧控制域包括帧类型、协议版本、发现路由、源路由、广播、地址、安全和保留位。

比特 0-1	2-5	6-7	8	9	10	11	12	13-13
帧类型	协议版本	发现路由	广播标记	安全	源路由	IEEE 目的地址	IEEE 源地址	保留

图 3-40 帧控制域结构

1）帧类型有数据、网络层命令和保留位。

2）协议版本为 ZigBee 网络层协议标准的版本号。

3）发现路由见网络层命令帧中的路由发现的介绍，包括抑制路由发现、使能路由发现、强制路由发现、保留。

4）广（多）播标志域为 1bit，如果是单播或者广播帧，值为 0，如果为多播帧值为 1。

5）安全域为该帧是否具有网络层安全操作能力，如果该帧的安全由另一层来完成或者完成被禁止，则该值是 0。

6）源路由子域值为 1 时，源路由子帧才在网络报头中存在。如果源路由子帧不存在则源路由子域值为 0。

7）IEEE 目的地址是 1 时，网络帧报头包含整个 IEEE 目的地址。

8）IEEE 源地址是 1 时，网络帧报头包含整个 IEEE 源地址。

（2）目的地址。在 ZigBee 网络层数据包中必须有目的地址域，其长度是 2 字节。如果帧控制域的多播标志子域值是 0，那么目的地址域值是 16 位的目的设备网络地址或者为广播地址。如果多播标志子域值是 1，目的地址域是 16 位目的多播组的 Group ID。值得注意的是设备的网络地址与 IEEE802.15.4—2003 协议中的 MAC 层 16 位短地址相同。

（3）源地址。在 ZigBee 网络层数据包中必须有源地址域，其长度是 2 字节，其值是源设备的网络地址。值得注意的是设备的网络地址与在 IEEE802.15.4—2003 协议中的 MAC 层 16 位短地址相同。

（4）广播半径域。广播域仅当目的地址为广播地址（0xFFFF）时，广播半径和广播序号存在。广播半径的长度为 1 字节，每个设备接收到一次该帧，则广播半径减 1。广播半径限定了传输半径范围。

（5）广播序列号域。在每个帧中都包含序列号域，其长度是 1 字节。每发送一个新的帧序列号值加 1。帧的源地址和序列号子域是一对，在限定了序列号 1 字节的长度内是唯一的标识符。

（6）IEEE 目的地址。如果存在 IEEE 目的地址域，则包含在网络层地址头中目的地址域的 16 位网络地址相对应的 64 位 IEEE 地址。如果该 16 位网络地址是广播或者多播地址，那么 IEEE 目的地址不存在。

（7）IEEE 源地址。如果存在 IEEE 源地址域，则包含在网络层地址头中的源地址域的 16 位网络地址相对应的 64 位 IEEE 地址。

（8）多点传送控制。多播控制域是 1 字节长度且只有多播标志子域值是 1 时存在。它分成 3 个子域，即多播模式（第 0、1 位，共 2 位）、非成员半径（第 2 ~ 4 位，共 3 位）、最大非成员半径（第 5 ~ 7 位，共 3 位）。多播模式（子域）表明无论是使用成员或非成员模式传输该帧。成员模式在目的组成员设备中使用传送多播帧。非成员模式是从不是多播组成员设备到是多播组成员设备换算多播帧。

当不是目的组成员设备转播时，非成员半径域表明成员模式多播范围。接收设备是目的组成员将设置该子域值是最大非成员半径（MaxNonmemberRadius）域的值。如果 NonmemberRadius field 的值是 0，接收设备不是目的组成员时将丢弃该帧，且如果 NonmemberRadius 域的值是在 0x01 到 0x06 范围内，那么将耗尽此域。如果 NonmemberRadius 域值是 0x07 表明无限的范围且不能被耗尽。

（9）源路由帧。如果帧控制域的源路由子域的值是 1，才存在源路由子帧域。它分成三个子域，即应答计数器（1 个字节）、应答索引（1 个字节）、应答列表（可变长）。

1）应答计数器子域表明包含在源路由子帧转发列表里的应答的数值。

2）应答索引子域表明传输的数据包的应答列表子域的下一转发的索引。这个域被数据包的发送设备初始化为 0，且每转发一次就加 1。

3）应答列表子域是节点的 2 字节短地址的列表，这个域用来为源路由数据包的目的转发。地址是最无意义字节格式且在源路由中有顺序地出现。

（10）帧有效载荷。帧有效载荷的长度是可变的，包含了各种帧类型具体信息。

3.2.2 传输方式选择

古代信息传递的方式包括：(1) 用候鸟，特别是鸽、雁等作传输工具。(2) 作内馅的方式，如把信息载体藏在鱼肚、饼类、包子中等。(3) 用特殊声音，如钟声、鼓声、鞭炮声等。(4) 用灯光、火光，如孔明灯、烽火台等。(5) 用其他记号、摆设等，如诱敌的记号。

现代信息传递方式包括：(1) 有线通信传输，如电话、传真、电报、电视等。(2) 无线通信传输，如对讲机、BP 机（已淘汰）、移动电话、收音机。(3) 数字通信传输，最熟悉的有，联网的电脑、数字电视。(4) 纸张通信传输，如书信、报纸等。(5) 钟鼓、烟火、鸽子、旗语、狼烟等方式传递信息。

无线数据的传递方式，若按被传输的数据信号的特点，可分为基带传输、频带传输和数字数据传输；若按数据传输的顺序可分为并行传输和串行传输；若按数据传输的同步方式可分为同步传输和异步传输；若按数据传输的流向和时间可分为单工、半双工和全双工传输。

下面从数据传输流向及时间分类来介绍无线数据传递方式。

(1) 单工方式（simplex mode）。通信双方在同一时刻只能单方向传送信息的一种通信方式。单工通信信道是单向信道，发送端和接收端的身份是固定的，发送端只能发送信息，不能接收信息；接收端只能接收消息，不能发送信息，数据信号仅从一端传送到另一端，如图 3-41 所示。



图 3-41　单工方式示意图

(2) 半双工方式。同一根传输线既作接收又作传送，虽然数据可以在两个方向上传送，但通信双方不能同时收发数据，如图 3-42 所示。采用半双工方式时，通信系统每一端的发送端和接收端，通过收、发开关转接到通信线上，进行方向的切换，因此会产生时间延迟。收、发开关实际上是由软件控制的电子开关。

半双工的系统可以比喻作单线铁路。若铁道上无列车行驶时，任一方向的车都可以通过。但若路轨上有车，相反方向的列车需等该列车通过道路后才能通过。

无线电对讲机就是使用半双工系统。由于对讲机传送及接收使用相同的频率，不允许同时进行。因此一方讲完后，需设法告知另一方讲话结束（例如讲完后加上“OVER”），另一方才知道可以开始讲话。

(3) 全双工方式。数据发送和接收分别由两根不同的传输线传送，通信双方都能在同一时刻进行发送和接收操作。在这种方式下，通信系统的每一端都设置了发送端和接收端，因此能控制数据同时在两个方向上传送，如图 3-43 所示。全双工方式无需进行方向的切换，因此没有切换操作所产生的时间延迟，这对那些不能有时间延误的交互式应用

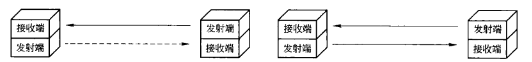


图 3-42　半双工方式示意图　　图 3-43　全双工方式示意图

(例如远程监测和控制系统) 十分有利。这种方式要求通信双方均有发送器和接收器，同时需要两根数据通路传送数据信号。

全双工的系统可以用一般的双向车道形容。两个方向的车辆因使用不同的车道，因此不会互相影响。

一般的电话、手机就是全双工的系统，因为在讲话时同时也可以听到对方的声音。

3.2.3 数据正确性校验

正确性是通信的一个重要指标，如果经过传输信息发生了改变或者是不能识别，那么无线通信也就失去了意义。

由于无线数据通信是以包的形式发送的，在无线数据传输过程中可能会出现包的丢失、损坏、重复等情况，为了保证无线数据正确传输，必须对数据包进行校验。

无线数据通信的数据包一般包括前导字符、地址、数据、校验码与结尾码等。校验码(可选) 主要用来对当前数据块进行校验，相同类型的设备一般也有相同的结尾码 (可选)。

为了确保接收方能收到正确的信息，引入了数据包的错误检测技术，发送方对所要发送的数据块进行计算，产生一个校验码，附加在有效信息的尾部。接收方根据约定对收到的数据重新计算其校验码，并与收到校验码进行对比，如果错误，一般丢弃该数据包，如果正确，则提交应用程序进行处理。

无线数据通信最简单的数据校验就是把原始数据和待比较数据直接进行比较，看是否完全一样，这种方法是最安全最准确的，同时也是效率最低的，适用于简单的数据量极小的通信。

目前无线数据通信使用校验码主要包括异或校验 (Xor)、累加和校验 (Add)、循环冗余校验 (Cyclic Redundancy Check，CRC)、累加和求补校验 (Check Sum) 等。

(1) 异或校验。异或校验码初始值为0，对待发送的信息以字节为单位，与初始值相异或，最后所得结果即为异或校验码，见表3-4。

表3-4 异或校验

A值	B值	Xor结果	A值	B值	Xor结果
0	0	0	0	1	1
1	0	1	1	1	0

(2) 累加和校验。累加和校验码初始值为0，对待发送的信息以字节为单位，与初始值相加模256，最后所得结果即为累加和校验码。

(3) 奇偶校验。奇偶校验码初始值是一个表示给定位数的二进制数中1的个数是奇数还是偶数的二进制数。奇偶校验位是最简单的错误检测码。奇偶校验位有两种类型，即偶校验位与奇校验位。如果一组给定数据位中1的个数是奇数，那么偶校验位就置为1，从而使得总的1的个数是偶数。如果给定一组数据位中1的个数是偶数，那么奇校验位就置为1，使得总的1的个数是奇数。

(4) 循环冗余校验。Xor校验与Add校验以字节为单位进行校验处理，算法比较简

单，容易出差错。CRC 算法比较复杂，其基本思想是将需要发送数据包当做一个巨大的二进制数，用它来除以一个固定二进制数，所得到余数即是求得的校验码，相对于 Xor 与 Add，其出错的概率很低。Xor 与 Add 校验的形式单一，而 CRC 由于所选用的多项式与原始值的不同，其算法也不尽相同，所得到的校验码结果也相异。

循环冗余校验码 CRC 全称是 Cyclic Redundancy Checksum。简单说它是一种利用二进制的多项式除法来取得数据的校验和的方法。

CRC 是两个字节数据流采用二进制除法相除所得到的余数。其中被除数是需要计算校验和的信息数据流的二进制表示；除数是一个长度为 $n+1$ 预定义（短）的二进制数，通常用多项式的系数来表示。在做除法之前，要在信息数据之后先加上 n 个 0。

CRCa 是基于有限域 GF（2）（即除以 2 的同余）的多项式环。简单来说，就是所有系数都为 0 或 1（又叫做二进制）的多项式系数的集合，并且集合对于所有的代数操作都是封闭的。例如：

$$(x^3 + x) + (x + 1) = x^3 + 2x + 1 \equiv x^3 + 1$$

2 会变成 0，因为对系数的加法运算都会再取 2 的模数，乘法也是类似的：

$$(x^2 + x)(x + 1) = x^3 + 2x^2 + x \equiv x^3 + x$$

同样可以对多项式作除法并且得到商和余数。例如如果用 $x^3 + x^2 + x$ 除以 $x+1$，会得到：

$$\frac{(x^3 + x^2 + x)}{(x + 1)} = (x^2 + 1) - \frac{1}{(x + 1)}$$

也就是说，

$$(x^3 + x^2 + x) = (x^2 + 1)(x + 1) - 1$$

这里除法得到了商 $x^2 + 1$ 和余数 -1，因为是奇数所以最后一位是 1。

字符串中的每一位其实就对应了这样类型的多项式的系数。为了得到 CRC，首先将其乘以 x^n，这里 n 是一个固定多项式的阶数，然后再将其除以这个固定的多项式，余数的系数就是 CRC。

在上面的等式中，$x^2 + x + 1$ 表示了本来的信息位是 111，$x + 1$ 是所谓的钥匙，而余数 1（也就是 $x0$）就是 CRC。key 最高次为 1，所以将原来的信息乘上 x 来得到 $x^3 + x^2 + x$，也可视为原来的信息位补 1 个零成为 1110。

一般来说，其形式为：

$$M(x) \cdot x^n = Q(x) \cdot K(x) + R(x)$$

式中，$M(x)$是原始的信息多项式；$K(x)$是 n 阶的“钥匙”多项式；$M(x) \cdot x^n$ 表示了将原始信息后面加上 n 个 0；$R(x)$是余数多项式，既是 CRC“校验和”。在通信中，发送者在原始的信息数据 M 后加上 n 位的 R(替换本来附加的0)再发送。接收者收到 M 和 R 后，检查 $M(x) \cdot x^n - R(x)$是否能被 $K(x)$整除。如果是，那么接收者认为该信息是正确的。值得注意的是 $M(x) \cdot x^n - R(x)$就是发送者所想要发送的数据。这个串又叫做 codeword。

CRCs 经常被叫做“校验和”，但是这样的说法严格来说并不是准确的，因为技术上来

说，校验“和”是通过加法来计算的，而不是 CRC 这里的除法。

“错误纠正编码”常常和 CRCs 紧密相关，其语序纠正在传输过程中所产生的错误。这些编码方式常常和数学原理紧密相关。

3.2.4 数据加密

在古代，保守一项秘密似乎要容易一些，因为只有少数人才有读书、写字的特权。如果一项秘密是书写下来的，那么只有数量极少的人才知道它是什么意思。通过限制人们学习书写文字，便可做到保密。然而这种保密机制显然具有很大的局限性。随着越来越多的人掌握了读写文字的能力，越来越有必要在这些人中间保守秘密。这种需要在战争期间愈发迫切。尽管真正打仗的人可能大多数都是文盲，但那些发动战争的人却并非如此。而且战争双方无疑都会雇佣一些能够读写敌方语言的士兵。古代战场上军队通信就是加密术的起源!

早期的加密方法非常简单。据说恺撒大帝曾用一种初级的密码来弄乱他传达的消息。对那些他认为能够分享秘密的人，便告诉他们如何重新组合回原来的消息。这种密码便是著名的“恺撒密码（The Caesar Cipher）”，如表 3-5 所示。它其实是一种简单的替换加密法：字母表中的每个字母依次都被靠后的第三个字母取代。换言之，字母 A 变成 D，B 变成 E，X 变成 A，Y 变成 B，Z 变成 C，依此类推。尽管这种加密术极易解码，但是“li brx grq'w nqrz krz lw'v qrw reylrxv!”转换成明文便是“if you don't know how it's not obvious!”（如果不知道原理，可也没那么简单!）。这种加密术的一个变种是 ROT-13 密码，每个字母均循环移动 13 个位置。

表 3-5 恺撒密码

明　码	密　码	明　码	密　码
A	B	⋮	⋮
C	E	R	P
B	A	S	T
D	F	⋮	⋮
E	K		

简单的替换加密存在重大的缺陷，因为重复出现的某个字母总是会用相同的字母替代。通过对某种语言的分析，便可知道字母被移位的大致距离——请注意上述密文中字母“r”的出现位置。熟悉英语的人就知道，它可能是一个元音——这种信息随即便可用来判断移位距离。

发展到近代，密码和与之对应的译码术在历史上占据了一个重要的地位。在美国被硬扯进入第二次世界大战之前，美国军方已有能力破解日本政府的密码。所以美国政府事实上能够事先知道日本攻击珍珠港的消息。然而，这一能力并未得到很好利用。由于这次“奇袭”，美国遭受了惨重的损失。

自恺撒大帝的年代开始，一直到当代，通信技术稳步地发展。从纸张到电报、电传、电话、传真以及电子邮箱，人和人之间的通信变得如此方便和普遍。与此同时，保障这些通信的安全也逐渐成为一项重要课题。最开始的时候，只有少数人关心此事，而且通常都是政府和军队。

每种通信方法的安全取决于建立通信的那种媒体（或媒介）。媒体越开放，消息落入外人之手就越有可能。现代通信方法一般都是开放和公用的。打一次电话或者发一次传真，信号会穿越一个共享的、公共的“电路交换”电话网络。而在发一次电子邮件的时候，它也会穿越一个共享的、公共的、包交换的网络。在网络中，位于通信双方两个端点之间的任何一个实体均可将消息（信号）轻易拦截下来。如果要通过现代的通信技术来进行数据的保密传输，便必须采用某种形式的加密技术，防范那些“偷窥者”窃取秘密，如图 3-44 所示。

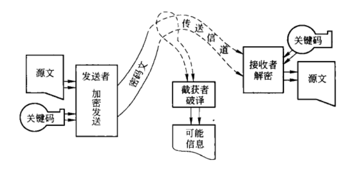


图 3-44 密码数据传递示意图

现代的基本加密技术要依赖于消息之目标接收者已知的一项秘密。通常解密方法（亦即“算法”）是任何人都知道的——就像所有人都知道怎样打开门一样。然而真正用来解开这一秘密的“密钥（key）”却并非尽人皆知——就像钥匙一样，一扇门的钥匙并不是任何人都拿得到的。当然还有某些加密系统建立在一种保密的算法基础上——通常把它叫做“隐匿保密”。但大多数人都讨厌使用这种加密方法，因为它未向公众开放。人们无从得知它的加密能力到底有多强，是否存在缺陷等（目前针对“加密芯片”展开辩论便是这样的一个例子）。

无线传输安全类似于通信安全。有各种各样的方法来发送一个信息。每一种方法都增强安全以保护信息的完整性。可以发送一张明信片，这样这个信息对于看到它的每一个人都是公开的。可以把这个信息放在信封里，防止有人随意看到它。如果确实要保证只有收件人能够看到这个信息，就需要给这个信息加密并且保证收件人知道这个信息的解码方式。

无线数据传输也是如此。没有加密的无线数据是在空中传输的，任何在附近的无线设备都有可能截获这些数据。

在无线传感网中一般采用的是 AES 加密算法。高级加密标准（Advanced Encryption Standard，AES）是一种迭代分组密码，采用的是代替、置换网络（SPN）。将明文分组长度固定为 128 位，而且仅支持 128、196 或 256 位的密钥长度。

AES 加密算法的实现包括密钥扩展过程和加密过程。加密过程又包括一个作为初始轮的初始密钥加法（AddRoundKey），接着进行 9 次轮变换（Round），最后再使用一个轮变换（FinalRound）。

大多数 AES 计算是在一个特别的有限域完成的。AES 加密过程在一个 4 × 4 字节矩阵上运作，这个矩阵又称为“体（state）”，其初值就是一个明文区块（矩阵中一个元素大

小就是明文区块中的一个 Byte）。加密时，各轮 AES 加密循环（除最后一轮外）均包含如下 4 个步骤：

（1）AddRoundKey 步骤。矩阵中的每一个字节都与该次循环的子密钥（round key）做 Xor 运算；每个子密钥由密钥生成方案产生。AddRoundKey 步骤，子密钥将会与原矩阵合并。在每次的加密循环中，都会由主密钥产生一把子密钥（透过 Rijndael 密钥生成方案产生），这把子密钥大小会跟原矩阵一样，以与原矩阵中每个对应的字节作异或加法，如图 3-45 所示。

（2）SubBytes 步骤。透过一个非线性的替换函数，用查找表的方式把每个字节替换成对应的字节，如图 3-46 所示。在 SubBytes 步骤中，矩阵中的各字节透过一个 8 位元的 S-box 进行转换。这个步骤提供了加密法非线性的变换能力。S-box 与 GF（28）上的乘法反元素有关，已知具有良好的非线性特性。为了避免简单代数性质的攻击，S-box 结合了乘法反元素及一个可逆的仿射变换矩阵建构而成。此外在建构 S-box 时，刻意避开了固定点与反固定点，即以 S-box 替换字节的结果会相当于错排的结果。

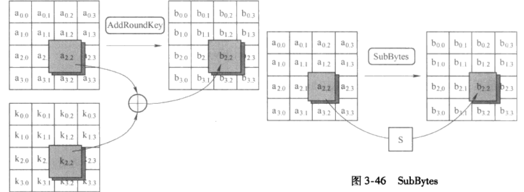


图 3-45　AES 计算

图 3-46　SubBytes

注：在 SubBytes 步骤中，矩阵中各字节被固定的 8 位查找表中对应的特定字节所替换 $b_{ij} = S(a_{ij})$

（3）ShiftRows 步骤。将矩阵中的每个横列进行循环式移位，如图 3-47 所示。

ShiftRows 是针对矩阵的每一个横列操作的步骤。在此步骤中，每一行都向左循环位移某个偏移量。在 AES 中（区块大小 128 位元），第一行维持不变，第二行里的每个字节都向左循环移动一格。同理，第三行及第四行向左循环位移的偏移量就分别是 2 和 3。128

图 3-47　ShiftRows

注：在 ShiftRows 步骤中，矩阵中每一行的各个字节循环向左方位移。位移量则随着行数递增而递增。

位元和 192 位元的区块在此步骤的循环位移的模式相同。经过 ShiftRows 之后，矩阵中每一竖列，都是由输入矩阵中的每个不同列中的元素组成。Rijndael 算法的版本中，偏移量和 AES 有少许不同；对于长度 256 位元的区块，第一行仍然维持不变，第二行、第三行、第四行的偏移量分别是 1 字节、2 字节、4 字节。

（4）MixColumns 步骤。为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每行内的四个字节，如图 3-48 所示。

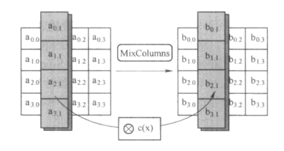


图 3-48 MixColumns

注：在 MixColumns 步骤中，每个直行都在 modulo x^4+1 之下和一个固定多项式 $c(x)$ 作乘法。

最后一个加密循环中省略 MixColumns 步骤，而以另一个 AddRoundKey 取代。

在 MixColumns 步骤中，每一直行的四个字节透过线性变换互相结合。每一直行的四个元素分别当作 1、x、x^2、x^3 的系数，合并即为 GF(2^8)中的一个多项式，接着将此多项式和一个固定的多项式 $c(x)=3x^3+x^2+x+2$ 在 modulox^4+1 下相乘。MixColumns 函数接受 4 个字节的输入，输出 4 个字节，每一个输入的字节都会对输出的 4 个字节造成影响。因此 ShiftRows 和 MixColumns 两步骤为这个密码系统提供了扩散性。

使用 32 或更多位元寻址的系统，可以事先对所有可能的输入建立对应表，利用查表来实现 SubBytes、ShiftRows 和 MixColumns 步骤以达到加速的效果。这么做需要产生 4 个表，每个表都有 256 个格子，一个格子记载 32 位元的输出；约占去 4KB（4096 字节）内存空间，即每个表占去 1KB 的内存空间。如此一来，在每个加密循环中，只需要查 16 次表，作 12 次 32 位元的 XOR 运算，以及 AddRoundKey 步骤中 4 次 32 位元 XOR 运算。

若使用的平台内存空间不足 4KB，也可以利用循环交换的方式一次查一个 256 格 32 位元的表。

3.2.5 典型两点间无线通信的实现

点对点无线通信是无线通信中最基本的方式，是点对多点无线通信以及无线网络的基础。点对点的通信，可以让读者了解无线通信的最基本技术环节，它们包含：配置无线芯片使之进入无线通信的准备状态；进入发送状态发送一个数据包；进入接收状态等待接收数据；查看发送数据是否发送成功。

在点对点的实验中，主要实现的功能有：发送模块上电复位后，进入无线通信的状态，并点亮红灯，表示进入无线发送状态，发送模块开始发送一个数据包，黄灯闪烁一

次；接收模块上电复位以后，进入无限通信状态，并点亮红灯，表示进入无线接收状态，接收到数据后黄灯闪烁一次，并将接收的数据通过串口发送给 PC（PC 软件是一个模拟的液晶程序，通过这个液晶程序可以了解液晶的使用方法）。整个点对点通信的框图如图 3-49所示。

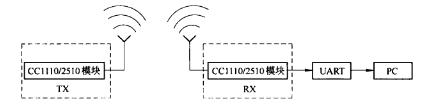


图 3-49 点对点通信系统框图

在点对点通信中，一共需要 RF 发送数据、RF 接收数据、串口函数和硬件配置函数等。下面将针对节点硬件对这些函数进行详细的讲解。

RF 配置函数是配置节点高频部分，该配置规定了无线收发器的收发频率、发送功率、无线传输速率、无线收发模式、调制方式以及数据长度等。下面就对节点进行配置，程序清单如下：

```
/ *******************************高频配置函数*****************************/
//函数名:BOOL halRfConfig(UINT32 frequency)
//输  入:频率
//输  出:无
//返  回:状态
/ ************************************************************************/
BOOL halRfConfig(UINT32 frequency)
{
  BOOL status;
  SET_MAIN_CLOCK_SOURCE(CRYSTAL); //打开主晶振
if(frequency == FREQUENCY_4_CC1110)          //判断频率
  {
    PA_TABLE0 = 0xC0;          //功率设置为 10dBm
    FREQ2 = 0x10;               //设置频段 433M
    FREQ1 = 0xAC;
    FREQ0 = 0x4E;
    //下面的配置通过 SmartRFStudio 高频软件中 CC1110 部分配置,
    //250 k 速率,GFSK 调制方式,540 kHz 接收滤波带宽. 配置频率范围是 433 MHz 或 868/915 MHz
    FSCTRL1 =   (frequency == FREQUENCY_4_CC1110) ? 0x0C : 0x12;
    FSCTRL1   = 0x12; //频率合成控制高位
    FSCTRL0   = 0x00; //频率合成控制低位
    MDMCFG4   = 0x2D; //调制解调配置
    MDMCFG3   = 0x3B;
    MDMCFG2   = 0x13;
```

```
    MDMCFG1   =0x22;
    MDMCFG0   =0xF8;
    DEVIATN   =0x62;  //调制解调背离配置(FSK 调制时使能).
    FREND1    =0xB6;
    FREND0    =0x10;
    MCSM0     =0x18;  //无线控制状态配置
    FOCCFG    =0x1D;  //频率偏移补偿配置
    BSCFG     =0x1C;  //位同步配置
    AGCCTRL2 =0xC7;  //AGC 控制
    AGCCTRL1 =0x00;
    AGCCTRL0 =0xB0;
    FSCAL3    =0xEA;  //频率合成校准
    FSCAL2 =   (frequency == FREQUENCY_4_CC1110)? 0x0A : 0x2A;
    FSCAL0    =0x1F;
    TEST2     =0x88;  //测试设置
    TEST1     =0x31;
    TEST0     =0x09;
    //校准合成器
    SIDLE();
    SCAL();
    while(MARCSTATE !  =0x01);
    INT_SETFLAG(INUM_RFTXRX,INT_CLR);
    status = TRUE;
    }
    else
    {
    status = FALSE;
    }
    return status;
}
```

RF 发送函数的功能是将待发送的数据通过无线的方式发送给另一个接收装置,当初始化完成以后,模块就进入了工作状态,在发送的过程中,它的数据长度是有限的,所以在发送的时候需要对数据的长度进行判断。程序清单如下:

```
/************************************************************************
描述:RF 发送数据
函数名:BYTE sppSend(SPP_STRUCT * pPacketPointer)
************************************************************************/
BYTE sppSend(SPP_STRUCT * pPacketPointer){
    BYTE res = TRUE;
    //检查发送数据的长度
    if(pPacketPointer- > payloadLength > SPP_MAX_PAYLOAD_LENGTH)
    {
```

```
        res = TOO_LONG;
        sppTxStatus = TX_IDLE;
    }
    if( ! (pPacketPointer->flags & RETRANSMISSION))
    {
        pPacketPointer->flags ^= SEQUENCE_BIT;
        pPacketPointer->payloadLength += SPP_HEADER_AND_FOOTER_LENGTH;
        pPacketPointer->srcAddress = myAddress;
    }
    //设置 DMA
    DMA_ABORT_CHANNEL(dmaNumberTx);
    SET_DMA_SOURCE(dmaTx,pPacketPointer);
    //如果信息长度正确就继续前进
    if(res == TRUE)
    {
        //清除 RF 中断标志和使能 RF 中断
        RFIF &= ~IRQ_DONE;
        RFIM &= ~IRQ_SFD;
        INT_SETFLAG(INUM_RF,INT_CLR);
        DMA_ABORT_CHANNEL(dmaNumberRx);
        SIDLE();
        RFTXRXIF = 0;
        INT_GLOBAL_ENABLE(FALSE);
        DMA_ARM_CHANNEL(dmaNumberTx);
        STX();
        INT_GLOBAL_ENABLE(TRUE);
        sppTxStatus = TX_IN_PROGRESS;
        if(pPacketPointer->flags & DO_ACK)
        {
            pAckData = pPacketPointer;
            waitForAck();
        }
        else
        {
            pAckData = NULL;
        }
        RFIM |= IRQ_DONE;
    }
    return res;
}
```

接收数据函数是接收同频率的发射机发送的数据，接收到的数据以后，需要返回一个状态以判断接收是否成功。程序清单如下：

```
/*************************************************************************
描述:RF 接收数据
函数名:void sppReceive(SPP_STRUCT * pReceiveData)
*************************************************************************/
void sppReceive(SPP_STRUCT * pReceiveData){
  sppRxStatus = RX_WAIT;                        //等待接收状态
  DMA_ABORT_CHANNEL(dmaNumberRx);
  SET_DMA_DEST(dmaRx,pReceiveData);
  SET_DMA_LENGTH(dmaRx,255);
  DMA_ARM_CHANNEL(dmaNumberRx);
  SIDLE();
  RFIF &= ~IRQ_SFD;
  RFIM |= IRQ_SFD;
  //进入接收状态
  SRX();
  return;
}
BOOL radioReceive(BYTE * * receiveData,BYTE * length,WORD timeout,BYTE * sender)
{
  BOOL status = TRUE;
  BOOL continueWaiting = TRUE;
  BOOL useTimeout = FALSE;
  if(timeout)
  {
    useTimeout = TRUE;
  }
  sppReceive(&rxData);                    //接收数据
  while((sppRxStatus != RX_COMPLETE)&&(continueWaiting))
  {
    if(useTimeout)                        //如果时间溢出接收失败
    {
      halWait(0x01);
      timeout--;
      if(timeout==0)
      {
        continueWaiting = FALSE;
        status = FALSE;
      }
    }
  }
  if(status == TRUE)                      //如果接收成功
  {
    * receiveData = rxData.payload;
```

```
    *length = rxData.payloadLength;
    *sender = rxData.srcAddress;
  }
  return status;                           //返回状态
}
```

点对点通讯 C51 源代码分为接收和发送两部分，前面的一些基本配置、初始化函数和功能函数都是相同的，模块的收发功能主要是在主函数里实现的。首先开始分析接收部分的函数。

接收部分的流程图如图 3-50 所示，接收模块主程序首先运行初始化程序，对 8051 的 CPU 和射频部分进行初始化，然后发光二极管红灯点亮后，表示系统进入等待状态。

程序中初始化了串行接口，UartTX_Send_String()函数使模块可以把模块从无线接收到的数据从串口发送出去。然后，程序进入接收等待状态，监视空气中的无线信号，判断是否有发送模块的数据包装，如果有，LED 状态取反和从串口输出接收到的数据。程序清单如下：

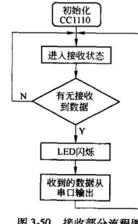


图 3-50 接收部分流程图

```
/*********************************************************************
描述:主函数
函数名:void main(void)
*********************************************************************/
#define  NOD_RX         1
void main(void)
{
  SET_MAIN_CLOCK_SOURCE(CRYSTAL);
  initUART();
  NOD_TO_NOD(NOD_RX);
}
/*********************************************************************
描述:模式选择
函数名:void NOD_TO_NOD(char sell)
*********************************************************************/
void NOD_TO_NOD(char sell)
{
  if(sell == 0)
  {
    myAddr = ADDRESS_0;                    //设置自己地址
    remoteAddr = ADDRESS_1;                //设置接收地址
    radioInit(frequency,myAddr);   //RF 初始化
    INT_GLOBAL_ENABLE(INT_ON);      //中断使能
    contionuousMode();              //连续发送模式
```

```
  }
  else if( sell == 1 )
  {
    myAddr = ADDRESS_1;                //设置自己地址
    remoteAddr = ADDRESS_0;            //设置接收地址
    radioInit( frequency, myAddr ); //RF 初始化
    INT_GLOBAL_ENABLE( INT_ON );      //中断使能
    receiveMode( );                  //接收模式
  }
}
/**********************************************************************
描述:接收模式
函数名:void receiveMode( void)
**********************************************************************/
void receiveMode( void)
{
  BYTE * receiveBuffer;
  BYTE length;
  BYTE res;
  BYTE sender;
#ifdef CC1110_NOD_RX
  unsigned char temp2[5] = {0x68,0xaa,'U','Y','J'};
#endif
  P1DIR |=0x02;
  while( ! stopApplication( ) )
  {
    res = radioReceive( &receiveBuffer,&length,RECEIVE_TIMEOUT,&sender) ;//接收数据
    if( res == TRUE)                          //接收成功
    {
      YLED = ! YLED;
#ifdef CC1110_NOD_RX
      Print_word( receiveBuffer,4,0,length-1) ;
      UartSendWord( temp2,5) ;
      UartSendWord( ( void * ) di_yz,sizeof( di_yz) ) ;
#endif
      }
      else
      {
        YLED = 1;
    }
  }
}
```

发送部分流程图如图 3-51 所示。发送模块主程序首先运行初始化程序，对 8051 的 CPU 和无线射频部分进行初始化。然后点亮红灯，表示系统进入等待状态。发送模块进入程序循环，然后调用 radioSend（BYTE * transmitData，WORD dataLength，BYTE remoteAddress，BYTE doAck）函数把 transmitData 缓冲区的数据发送出去后，相应的黄色 LED 闪烁一次。程序清单如下：

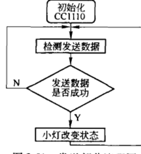


图 3-51 发送部分流程图

```
#define NOD_TX        0
/******************************************************************************
描述:主函数
函数名:void main(void)
******************************************************************************/
void main(void)
{
  SET_MAIN_CLOCK_SOURCE(CRYSTAL);
  while(1)
  {
    NOD_TO_NOD(NOD_TX);                    //选择发送部分
  }
}
/******************************************************************************
描述:模式选择
函数名:void NOD_TO_NOD(char sell)
******************************************************************************/
void NOD_TO_NOD(char sell)
{
  if(sell ==0)
  {
    myAddr = ADDRESS_0;                //设置自己地址
    remoteAddr = ADDRESS_1;            //设置接收地址
    radioInit(frequency,myAddr);  //RF 初始化
    INT_GLOBAL_ENABLE(INT_ON);     //中断使能
    contionuousMode();                 //连续发送模式
  }
  else if(sell == 1)
  {
    myAddr = ADDRESS_1;                //设置自己地址
    remoteAddr = ADDRESS_0;            //设置接收地址
    radioInit(frequency,myAddr);  //RF 初始化
    INT_GLOBAL_ENABLE(INT_ON);     //中断使能
    receiveMode();                     //接收模式
```

```
    }
}
/***********************************************************************
描述:连续发送模式
函数名:void contionuousMode(void)
************************************************************/
void contionuousMode(void)
{
    BOOL res;
    int i =0;
    BYTE sendBuffer1[ ] = "hello world";            //发送的数据设置
    BYTE sendBuffer2[ ] = "hello CDWXL";
    P1DIR |=0x02;
    while(1){
      if(i ==0)
      {
        res = radioSend(sendBuffer1,sizeof(sendBuffer1),remoteAddr,DO_ACK);//发送数据
        i ++;
      }
      else
      {
        res = radioSend(sendBuffer2,sizeof(sendBuffer2),remoteAddr,DO_ACK);//发送数据
        i =0;
      }
      if(res == TRUE)                                   //发送成功
      {
            YLED = ! YLED;
      }
      else
    {
            YLED = 1;
    }
    halWait(200);
    halWait(200);
  }
}
```

3.3　无线传感网需要的基本技术

无线传感网中无线通信与有线通信在诸多重要环节上完全不同，这些环节中的异同导致了它们之间通信质量的差异：

（1）无线链路通过相同的传输媒介——空气来传播无线电信号。

（2）误码率比常规有线系统高几个数量级。由于存在上述差异，RF 链路的可靠性比

有线链路低。

(3) 为了实现在同一范围内多点间通信，必须考虑防止数据包在空气中传输时相互碰撞，为了建立可靠的无线传输通路，必须采用各种方法。例如TDMA/FDMA/CSMA等都是无线通信中常用的办法。

3.3.1 基本抗冲突技术

3.3.1.1 FDMA

FDMA（Frequency Division Multiple Access）是数据通信中的一种技术，即不同的用户分配在时隙相同而频率不同的信道上，如图3-52所示。按照这种技术，把在频分多路传输系统中集中控制的频段根据要求分配给用户。同固定分配系统相比，频分多址使通道容量可根据要求动态地进行交换。

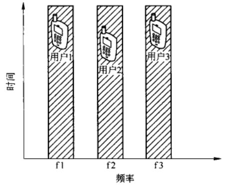


图3-52 FDMA

在FDMA系统中，分配给用户一个信道，即一对频谱，一个频谱用作前向信道即基站向移动台方向的信道，另一个则用作反向信道即移动台向基站方向的信道。这种通信系统的基站必须同时发射和接收多个不同频率的信号，任意两个移动用户之间进行通信都必须经过基站的中转，因而必须同时占用两个信道（两对频谱）才能实现双工通信。

以往的模拟通信系统一律采用FDMA。频分多址（FDMA）是采用调频的多址技术。业务信道在不同的频段分配给不同的用户。如TACS系统、AMPS系统等。频分多址是把通信系统的总频段划分成若干个等间隔的频道（也称信道）分配给不同的用户使用。这些频道互不交叠，其宽度应能传输一路数字话音信息，而在相邻频道之间无明显的串扰。

频分多址（FDMA）技术将可用的频率带宽拆分为具有较窄带宽的子信道，如图3-50所示。这样每个子信道均独立于其他子信道，从而可被分配给单个发送器。其优点是软件控制上比较简单，其缺陷是子信道之间必须间隔一定距离以防止干扰，频带利用率不高。

FDMA是指不同的节点占用不同的频率，即每个节点占用一个频率的信道进行通话或通信。因为各个节点使用不同频率的信道，所以相互没有干扰。这是模拟载波通信、微波通信、卫星通信、蜂窝式移动电话的基本技术，也是第一代模拟移动通信的基本技术，早期的移动通信多使用这种方式。由于每个节点进行通信时占用一个频率、一个信道，频带利用率不高。随着通信技术的迅猛发展，很快就显示出其容量不足的缺点。

FDMA是一个多频率的通信方式，在设计中频段的改变是必要的，将频段设置为433MHz，要改变信道的方法是改变寄存器CHANNR，在改变信道的时候，只需要改变CHANNR的值，在下面的代码中给出了两个设备选择不同信道的方法。

```
if( state ==0)
        CHANNR    =0x00;
    else
        CHANNR    =0x01;
```

在实验中，使用三个无线通信模块，两个发送模块 TX1 和 TX2，一个接收模块 RX，如图 3-53 所示。当发送模块有按键按下时，发送模块就会向接收模块发送数据，直到发送成功或者超时退出。

模块 TX1 和模块 TX2 在编程时，被强制固定在不同的子频道上，模块 TX1 和模块 TX2 同时向 RX 模块发送数据包（因为在不同的子频道上发射，所以在空气中，这些数据包不会发生碰撞，不会出现数据包的传输错误）。而 RX 模块时时刻刻地扫描监视空气中不同子频道，发现有合格的数据包，就会自动进行接收。这就实现了点（RX 模块）对多点（模块 TX1 和模块 TX2）的可靠无线数据通信。

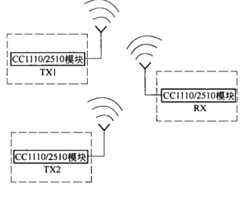


图 3-53 FDMA 通信框图

在日常生活中使用的手机、工业控制的无线系统、无线传感器系统都是采用 FDMA 的无线通信传输方式。

3. 3. 1. 2 TDMA

时分多址（Time Division Multiple Access，TDMA）是把时间分割成周期性帧（Frame），每一个帧再分割成若干个时隙向基站发送信号，在满足定时和同步的条件下，基站可以分别在各时隙中接收到各移动终端的信号而不混扰。同时基站发向多个移动终端的信号都按顺序安排在预定的时隙中传输，各移动终端只要在指定的时隙内接收，就能在合路的信号中把发给它的信号区分并接收下来。

TDMA 较之 FDMA 具有通信信号质量高，保密较好，系统容量较大等优点，但它必须有精确的定时和同步以保证移动终端和基站间正常通信，技术上比较复杂。

TDMA 是在同一个信道上，把不同地址发送的信号按照时间间隔的方法进行传输的一种无线通信方式。图 3-54 所示为通信示意图。

TDMA 是在一个信道上对时间进行分配，让设备在不同的时间中完成数据的交互通信。模块 TX1 和模块 TX2 在编程时，程序的写法是完全相同的，模块 TX1 和模块 TX2 不断检测按键，如果有按键按下，发送模块（以后称为节点模块）就开始接收模块（以后称为主机）定时发送出来的同步信号。收到同时信号后，就产生一个与自己 ID 相关的延时函数后直接把按键值发送出去。而主机每时每刻自动扫描监视空气中的信号并在一定时间内发送一次同步信号，发现有合格的数据包，就会自动进行接收。这就实

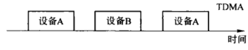


图 3-54 TDMA 通信示意图

现了点（主机模块）对多点（节点1和节点2）的可靠无线数据通信。很多工业控制的无线系统，无线传感器系统，很多都采用TDMA的无线通信传输方式。

3.3.1.3 CSMA

CSMA/CD是英文“Carrier Sense Multiple Access Collision detect”的缩写，中文的意思是“载波监听多路访问（冲突）/检测”，其工作原理如下：

（1）若媒体空闲，则传输；

（2）若媒体忙，一直监听直到信道空闲，然后立即传输；

（3）若在传输中监听到干扰，则发干扰信号通知所有站点。等候一段时间，再次传输。

以上原理可以通俗理解为：“先听后说，边说边听”。CSMA/CD是一种分布式介质访问控制协议，网中的各个站（节点）都能独立地决定数据帧的发送与接收。每个站在发送数据帧之前，首先要进行载波监听，只有介质空闲时，才允许发送帧。这时，如果两个以上的站同时监听到介质空闲并发送帧，则会产生冲突现象，这使发送的帧都成为无效帧，发送随即宣告失败。每个站必须有能力随时检测冲突是否发生，一旦发生冲突，则应停止发送，以免介质带宽因传送无效帧而被白白浪费，然后随机延时一段时间后，再重新争用介质，重发送帧。CSMA/CD协议简单、可靠，其网络系统（如Ethernet）被广泛使用。

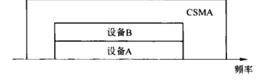


图3-55 CSMA原理

载波监视（如图3-55所示）这种无线通信方式比起前面介绍的FDMA和TDMA来，它能更好地利用资源。因为这种通信方法在发送数据之前，一直在检测空气中是否存在有相同频率的载波，如果在当前时间空气中有相同频率的载波，就不发送数据。如果空气中没有同频率的载波，表明现在空间资源没有被占用，可以发送数据，这样不仅提高了空间资源的利用效率，也提高了通信的可靠性。

主机（接收端）程序非常简单，可直接采用点对点实验中的发送接收函数完成数据的通信，与之不同的是，发送的部分采用两个，也就是说有两个发送模块同时工作，并且它们的频率、发送的方法都完全一致。但是为了体现它们之间的差异，将两个模块发送的数据做适当的修改，在发送模块1中发送的数据定义为“hello world”，发送模块2中发送的数据定义为“hello CDWXL”。载波监听部分的代码添加到发送函数中，所以接收部分的程序和点对点程序完全相同。初始化完成之后，程序进入主循环程序。模块开始载波监听，当检测到空气中没有相同载波数据的时候，便发送相应的数据，各个模块采用竞争的方式发送。收到节点发送过来的数据后，通过串口显示出来。

3.3.2 基本抗干扰技术

跳频通信（FHSS）可以说是抗干扰能力最强的一种通信方式，如图3-56所示，其实它的原理和上面讲的CSMA的原理近似。但与CSMA通信方式比较，跳频通信的灵活性更大，能够更加合理地利用空间资源。在跳频的通信过程中，发送端如果在发送了数据包

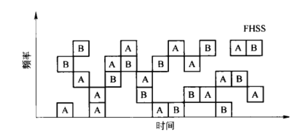


图 3-56 FHSS 通信示意图

后，在一定的时间内没有回复，那就说明空气中有相同频率的载波存在，不会像 CSMA 遇到这样的情况就进入了等待状态，跳频中这时就更换频道了，继续尝试有没有回复，如有回复就说明通信成功。这样就可以容易地实现接收和发送端的跳频节奏一致，这样就把通信范围从一个频道扩展到了另一个频谱上。

在跳频通信过程中主要是看如何实现接收和发送端在改变频道的过程中实现频道的统一，而且在频道转换过程中应当尽可能地少花费时间。FHSS 和 FDMA 一样是一个多频率的通信方式，在实验中信道的改变是必要的，将频段设置为 2.4GHz，要改变信道的方法是改变寄存器 CHANNR，在改变信道的时候，只需要改变 CHANNR 的值，在下面的代码中给出了两个设备选择不同信道的方法。

```
if( ++CHANNR_Number ==6) CHANNR_Number =0;
radioInit(frequency,myAddr,CHANNR_Number);
```

上面的函数就是配合跳频数组来改变频道用的，在这里只要确定节点是工作在发送状态或是工作在接收状态之后，就可以确定它的频道，而在通讯的过程中可以不断地调整频道来进行通信。在这里只用到了 6 个频道，其实在应用中可以适当地增加或减少所用的频道。

3.3.2.1 直接序列扩频（DSSS）

直接序列扩频（DSSS）技术是当今人们所熟知抗干扰的扩频技术之一。它是“二战”期间开发的，最初的用途是为军事通信提供安全保障。直接序列扩频技术将窄带信息信号扩展成宽带噪声信号。这种技术使敌人很难探测到信号，即便探测到信号，如果不知道正确的编码，也不可能将噪声信号重新汇编成原始的信号。

由于它抗噪声的特性，直接序列扩频技术也非常适合商业应用。在容许无线设备公开使用的电磁环境里，它对其他传统微波设备造成最小的干扰，同时对附近其他设备有更高的抗扰性。20 世纪 80 年代末，晶体电子技术的先进程度已经足以提供商用的、成本效益好的直接序列扩频系统。

直接序列扩频 DSSS（Direct Sequence Spread Spectrum）是直接利用具有高码率的扩频码系列采用各种调制方式在发端与扩展信号的频谱，而在收端，用相同的扩频码序去进行解码，把扩展宽的扩频信号还原成原始的信息。它是一种数字调制方法，具体说，就是将信源与一定的 PN 码（伪噪声码）进行模二加。例如说在发射端将“1”用 11000100110，而将“0”用 00110010110 去代替，这个过程就实现了扩频，而在接收端处只要把收到的序列是

11000100110 就恢复成“1”，是 00110010110 就恢复成“0”，这就是解扩。这样信源速率就被提高了 11 倍，同时也使处理增益达到 10dB 以上，从而有效地提高了整机倍噪比。

直接序列扩频技术通过将射频载波和伪噪声（PN）数字信号有效地相乘来执行数据处理。首先，它通过相应的调制手段（如 BPSK、QPSK、QAM 等）将 PN 码调制到信息信号上。然后，用一个双重平衡混频器将射频载波和经 PN 码调制的信息信号相乘。

这种数据处理方法将射频信号替换成一个与噪声信号频谱相同的，但带宽很宽的信号。在接收端，它将接收的射频信号与同一个经 PN 码调制的载波相乘来进行解调。解调后输出一个接收端的射频信号。这解调的射频信号和噪声信号的功率最接近时它的功率最高，并且和信道的噪声最“相关”（Correlated）。然后，将这“相关”的信号过滤、解调，就可以恢复初始数据。

由于 PN 码的带宽很宽，所以可在不丢失信息的情况下，将信号能量降低到噪声限度以下：通常将功率输出频谱主瓣的零值到零值（null to null）的带宽（2Rc）（Rc 是码片率）认定为直接序列扩频系统的带宽。应该注意的是，扩频主瓣中包含的能量构成了扩频信号 90% 以上的总能量。因此容许在较窄的射频带宽里把接收信号还原为清晰的时域脉冲信号。

A 直接序列扩频通讯的优点

直扩系统射频带宽很宽。小部分频谱衰落不会使信号频谱严重畸变。

多径干扰是由于电波传播过程中遇到各种反射体（高山、建筑物）引起，使接收端接受信号产生失真，导致码间串扰，引起噪声增加。而直扩系统可以利用这些干扰能量提高系统的性能。

直扩系统除了一般通信系统所要求的同步以外，还必须完成伪随机码的同步，以便接收机用此同步后的伪随机码去对接受信号进行相关解扩。直扩系统随着伪随机码字的加长，要求的同步精度也就高，因而同步时间就长。

直扩和跳频系统都有很强的保密性能。对于直扩系统而言，射频带宽很宽，谱密度很低，甚至淹没在噪声中，就很难检查到信号的存在。由于直扩信号的频谱密度很低，直扩系统对其他系统的影响就很小。

直扩系统一般采用相干解调解扩，其调制方式多采用 BPSK、DPSK、QPSK、MPSK 等调制方式。而跳频方式由于频率不断变化、频率的驻留时间内都要完成一次载波同步，随着跳频频率的增加，要求的同步时间就越短。因此跳频多采用非相干解调，采用的解调方式多为 FSK 或 ASK，从性能上看，直扩系统利用了频率和相位的信息，性能优于跳频。

B 直接序列扩频通信技术的特点

直接序列扩频通信技术具有如下特点：

（1）抗干扰性强。抗干扰是扩频通信的主要特性之一，比如信号扩频宽度为 100 倍，窄带干扰基本上不起作用，而宽带干扰的强度降低了 100 倍，如要保持原干扰强度，则需加大 100 倍总功率，这实质上是难以实现的。因信号接收需要扩频编码进行相关解扩处理才能得到，所以即使以同类型信号进行干扰，在不知道信号的扩频码的情况下，由于不同扩频编码之间的不同的相关性，干扰也不起作用。正因为扩频技术抗干扰性强，美国军方在海湾战争等处广泛采用扩频技术的无线网桥来连接分布在不同区域的计算机网络。

（2）隐蔽性好。因为信号在很宽的频带上被扩展，单位带宽上的功率很小，即信号功率谱密度很低，信号淹没在白噪声之中，别人难以发现信号的存在，加之不知扩频编码，

很难拾取有用信号，而极低的功率谱密度，也很少对于其他电信设备构成干扰。

（3）易于实现码分多址（CDMA）。直扩通信占用宽带频谱资源通信，改善了抗干扰能力，但是否浪费了频段？其实正相反，扩频通信提高了频带的利用率。正是由于直扩通信要用扩频编码进行扩频调制发送，而信号接收需要用相同的扩频编码作相关解扩才能得到，这就给频率复用和多址通信提供了基础。充分利用不同码型的扩频编码之间的相关特性，分配给不同用户不同的扩频编码，就可以区别不同用户的信号，众多用户，只要配对使用自己的扩频编码，就可以互不干扰地同时使用同一频率通信，从而实现了频率复用，使拥挤的频谱得到充分利用。发送者可用不同的扩频编码，分别向不同的接收者发送数据；同样，接收者用不同的扩频编码，就可以收到不同的发送者送来的数据，实现了多址通信。美国国家航天管理局（NASA）的技术报告指出：采用扩频通信提高了频谱利用率。另外，扩频码分多址还易于解决随时增加新用户的问题。

（4）抗多径干扰。无线通信中抗多径干扰一直是难以解决的问题，利用扩频编码之间的相关特性，在接收端可以用相关技术从多径信号中提取分离出最强的有用信号，也可把多个路径来的同一码序列的波形相加使之得到加强，从而达到有效的抗多径干扰。

（5）直扩通信速率高。直扩通信速率可达 2M、8M、11M，无需申请频率资源，建网简单，网络性能好。在 802.15.4 通讯标准中，要求的无线通讯的速度是 250KB/s，所以，CC2430、CC2431 高频部分也是使用这个通讯速度。

C　直接序列扩频系统的处理增益

在发射机端，通过使用伪随机噪声码片序列，将窄带调制信号的带宽扩大（至少 10 倍）。直接序列扩频信号的生成（扩展）扩频传输的主要特色是：窄带信号和扩频信号中，两者的射频功率和承载的信息都相同。但是在扩频信号里，由于窄带信号的功率被分解在扩宽了的信道，扩频信号的功率密度比窄带信号的功率密度小得多。因此，要探测到扩频信号比探测到窄带信号的难度要大得多。功率密度是信号在某个频率区间里的平均功率。在这个例子中，假定扩展比是 11，那么，窄带信号的功率密度比扩频信号的功率密度大 11 倍。这个例子中使用 11 个芯片，是因为它符合 FCC 第 15 部分关于最小处理增益的规定。在接收端，扩频信号被解扩后，被还原为原始的窄带信号：如果同一频带设备在邻近同时使用，便会引起干扰（同频干扰）。

一个直扩系统在扩频、解扩过程中，干扰信号将同时被扩展，因而大大降低了干扰的影响。这就是直接序列扩频设备的抗干扰能力的来源。干扰信号至少被扩展了 10 倍（扩展系数）。也就是说，干扰信号的幅度被大大降低了，至少降低 90%。这就是直接序列扩频系统的“处理增益系数”。它等于传输带宽与信号带宽的比：$G_p = BW_t / BW_i$。

处理增益还取决于所用的伪随机噪声序列（PN 序列）中的码片数。PN 序列的范例有 M 序列和巴克序列，Wi-Lan 的直接序列扩频产品中都使用了这两种序列。这些 PN 序列都具有优良的自相关特性和交叉相关特性。

D　直接序列扩频技术和多径问题

直接序列扩频技术还因它的抗多径干扰性能而闻名。多径干扰导致信号的衰落、抖动和分解。这是在市区应用的室内或室外无线电通信技术固有的问题，因为金属设备和建筑物结构很容易反射射频信号而形成干扰。这些反射使接收信号包含了多个不同传送路径的折射信号，这些折射波到达接收端的时间不同而做成多径干扰。标准的 DSSS 接收机用一

个相关器（Correlator）自动选择幅度最大的折射波，并与之锁定同步。这样可以把多径干扰大大地降低。倾斜的 Rake DSSS 接收机不仅减小了多径效应，同时更优化了无线电设备的性能。Rake DSSS 接收机可以使不同的折射波重新同步，并将它们组合起来，大大提高了接收信号的清晰度和强度。

E 直接序列扩频与窄带相比的优点

（1）低功率频谱密度。因为信号被扩展到一个宽频带上，功率频谱密度很低，不易被探测到。

（2）对其他系统没有干扰或干扰很小。因为它的功率频谱密度很低，所以邻近的通信系统不会受到很强的干扰（不过，高斯噪声水平增加了）。在所有情况下，都使用整个频谱；因此干扰的情况比较恒定。

（3）随机码难以识别，保护用户隐私。只有发射机和接收机能够识别所应用的 PN 码。这就意味着，几乎不可能译解另一用户的信息。

（4）应用扩频技术，降低多径干扰。这取决于所使用的 PN 码的特性。

（5）解决同区使用（co-location）的问题。只要系统使用正交的扩频码，即可在同地区使用而不受同频干扰的限制。

上面的讨论，涉及很多无线通讯和数据通讯的基本原理和基础知识，对于刚刚进入这个新领域的单片机工程师和电子工程师，不一定能很快完全理解，但从上面的讨论，已经了解到了直接序列扩频的简单原理和在抗干扰、兼容和符合 FCC 的要求，高可靠性无线通信方面的显著优点，这就是很大的收获，由于这些高频电路已经完全集成到了芯片内部，要做的，只是用 C51 工具进行应用软件开发。通过对若干寄存器的控制，就能很容易地在实际应用中，使用先进的直接序列扩频无线通信技术了。

3.3.2.2 载波侦听多点接入/冲突检测（CSMA/CA）

知道总线型局域网在 MAC 层的标准协议是 CSMA/CD，即载波侦听多点接入/冲突检测（Carrier Sense Multiple Access with Collision Detection）。但由于无线产品的适配器不易检测信道是否存在冲突，因此 802.15 全新定义了一种新的协议，即载波侦听多点接入/避免冲撞 CSMA/CA（with Collision Avoidance）。一方面，载波侦听——查看介质是否空闲；另一方面，避免冲撞——通过随机的时间等待，使信号冲突发生的概率减到最小，当介质被侦听到空闲时，优先发送。不仅如此，为了系统更加稳固，802.15 还提供了带确认帧 ACK 的 CSMA/CA。在一旦遭受其他噪声干扰，或者由于侦听失败时，信号冲突就有可能发生，而这种工作于 MAC 层的 ACK 此时能够提供快速的恢复能力。

以太网属于广播形式的网络，当一个站点发送信息时，网络中的所有站点都能接收到，容易形成数据堵塞，导致网络速度变慢，甚至发生系统瘫痪。为了尽量减少数据的传输碰撞和重试发送。以太网中使用了 CSMA/CA（载波监听多路访问/冲突检测）工作机制。以防止各站点无序地争用信道。无线局域网中采用了与 CSMA/CD 相类似的 CSMA/CA（载波监听多路访问/冲突防止）协议，当其中一个站点要发送信息时。首先监听系统信道空闲期间是否大于某一帧的间隔。若是，立即发送，否则暂不发送，继续监听。CSMA/CA通信方式将时间域的划分与帧格式紧密联系起来，保证某一时刻只有一个站点发送，实现了网络系统的集中控制。

因为传输介质的不同，所以传统的 CSMA/CD 与无线局域网中的 CSMA/CA 在工作方式上存在着差异。CSMA/CD 的检测方式通过电缆中电压的变化来测得，当数据传输发生碰撞时，电缆中的电压就会随着发生变化，而 CSMA/CA 使用空气作为传输介质。必须采用其他的碰撞检测机制。CSMA/CA 采取了三种检测信道空闲的方式，即能量检测（ED）、载波检测（CS）和能量载波混合检测。

（1）能量检测（ED）：接收端对接收到的信号进行能量大小的判断，当功率大于某一确定值时，表示有用户在占用信道，否则信道为空。

（2）载波检测（CS）：接收端将接收到的信号与本机的伪随机码（PN 码）进行运算比较，如果其值超过某一极限时，表示有用户在占用信道，否则认为信道为空。

（3）能量载波检测：它是能量检测和载波检测两种工作方式的结合。

在 IEEE802.15.4 CSMA/CA 机制中，网络协调器在网络中会发出信标给所有的可感应节点，而对于有数据需传送的设备来说，它们会向网络协调器要求进行传送。由于在一段时间内只能有一个设备进行传输，因此所有想要传输的节点设备就会通过 CSMA/CA 机制来竞争传输媒体的使用权。所有准备传输数据的设备，会监测目前的无线传输媒体是否有其他设备在使用中，如果为空闲，此时，这些设备会产生一个倒退延迟时间，来错开这些设备同时送出数据从而造成碰撞的可能。若目前的无线传输媒体是忙碌中的，则这些设备将会在监测到媒体为空闲后，再进行 CSMA/CA 的竞争。

在 IEEE802.15.4 CSMA/CA 算法中，CSMA/CA 算法（如图 3-55 所示）是用于节点间数据传输时的信道争用机制，此算法中有三个重要的参数由每个要传送数据的设备去维护，即 *NB*、*CW* 和 *BE*。

（1）*NB*（后退次数，Number of Back）：*NB* 的初始值为 0，当设备有数据要传送时，经过一段后退时间后，发送 CCA 检测，若检测到信道忙，则会再一次产生倒退时间，此时 *NB* 值会加 1，在 IEEE802.15.4 中，*NB* 值最大定义为 4，当信道在经过 4 次的后退延迟时间后仍为忙，刚放弃此次的传送，以避免过大开销。

（2）*CW*（碰撞窗口的长度，Content Window Length）：也就是后退延迟时间的长度，单位是 Backoff，一个后退周期的定义在 MAC PIB 中由参数 aUnitBackofPeriod 给出，为 20symbol 的时间。*CW* 的初始值为 2，最大值为 31。

（3）*BE*（后退指数，Backoff Exponent）：取值范围为 0~5，15.4 推荐的默认值为 3，最大值为 5。当 *BE* 设为 0 时，则只进行一次碰撞检测。在 IEEE802.15.4 中，失败的次数（重传）最多 3 次。图 3-57 所示是 CSMA/CA 算法流程，其中在步骤（3）是完成 CCA 的部分。

3.3.3　一个简单星状网络实现简单数据通信

无线网络是由一个主机和若干个网络节点所组成（见图 3-58）。采用星状网络拓扑，主机可以向所有节点发送广播信号，也可以单独发送数据给一个指定的节点，同时知道现在在网络中节点的个数。所有的节点都可以随时加入或退出网络，在网络中的节点可以向中心发送自己的数据，该网络最重要的特点是具有网络自组织、自管理功能。

整个网络由一个主机和若干个网络节点组成。整个网络必须要运行在同一个时钟系统上，才能达到有序不断的工作状态。现在把网络分成五个时段，每一个时段分配一定的时间。五个时段依次为：网络同步时段、加入退出网络时段、广播信号时段、网络维持及数

CSMA/CA

$NB=0, CW=2$

电池是否用完

Y

BE=最小值（2、macMinBE）

N

BE=macMinBE

设置后退周期

随机延迟从(2BE-1)到后退周期

在后退周期内完成的CCA

信道是否空闲

Y

N

$CW=2, NB=NB+1, BE=\min(BE+1, \text{amax}BE)$

$CW=CW-1$

N

N

$NB>$macMaxCSMA后退

$CW=0$

Y

Y

失败

成功

图 3-57 CSMA/CA 算法流程

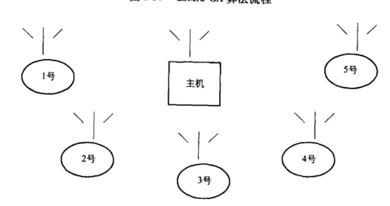


图 3-58 无线数据传输网络系统框图

据交换申请时段、点对点数据交换时段。各个时段功能及说明如下：

（1）网络同步时段。网络同步是为了让主机和所有的节点都处于同一时钟系统上。因为主机和节点都有各自的定时器，所以可以利用定时器让所有工作状态同步，但是为了消除误差，所以每隔一定时间就进行一步同步及定时器的校准。主机在同步时段发送同步信号，而所有节点在同步时段都进入接收状态，接收主机发送的同步信号然后进行校准。

（2）加入退出网络时段。加入退出网络时段是为了让新的节点加入网络和一些在网络中的节点退出网络而设定的。一个节点想要向主机发送数据，节点必须要在网络中，才能与主机进行数据交换。主机在此时段一直处于接收状态，接收节点发送过来的加入网络信号和退出网络信号，然后给予应答。节点方面，新的节点会在收到同步信号之后向主机发送加入网络信号，在网络中的节点想要退出网络也在此时向主机发送退出网络信号。

（3）广播信号时段。广播信号时段是主机有广播数据时，以广播的形式发送广播信号，所有在网络中的节点都可以接收到广播信号。同时这个时段也是主机向网络中单一的节点发送数据的时段，所有的节点在此时处于接收状态，无论是主机发送的广播信号还是发送给单一节点的数据，所有节点都可以收到，节点会自动判断是广播信号还是发送给单一节点的信号而做出响应。如果是单一发给自己的数据，节点收到数据后会马上发送应答信号。

（4）网络维持及数据交换申请时段。网络维持及数据交换申请时段可以对网络进行维持，所有在网络中的节点都会在这个时段向中心发送网络维持信号，以表示自己工作正常。同时也是节点向中心发送申请有大量数据要传送给主机的申请信号，通知主机在下一个点对点数据交换时段来索取数据。在此时段，主机随时工作在接收状态，各个节点以时分的方式向主机发送网络维持信号或数据申请交换信号。主机在收到每个节点的网络维持及数据交换申请信号后都会马上发送应答信号。

（5）点对点数据交换时段。点对点数据交换时段是在网络维持及数据交换申请时段中有的节点申请数据交换后，主机向那些节点索取数据的时段。当节点有大量的数据想传给中心，为了不占用其他节点跟主机通信的实时性，所以都统一在这个时段向主机发送数据。在这个时段，主机依次访问在网络维持及数据交换申请时段中申请过有数据发送的节点。所有的节点都处于接收状态，接收到主机索取数据的信号后，如果与自己的地址匹配就立即发送要上传的数据。

3.3.3.1 网络同步时段

主机程序为主机连续发送三次同步信号（即自己定时器的值和状态计数器的值），可让从机收到后纠正自己的定时器的计数值和状态计数器的值。此处设定同步信号的帧头为：0xdd。

主机程序如下：

```
while(j<3)
{
    TR0 = 0;          //读寄存器信息
    Th = TH0;
```

```
    Tl = TL0;
    TR0 = 1;
    TxBuf[0] = 0xdd;  //装包同步信号
    TxBuf[1] = Th;
    TxBuf[2] = Tl;
    TxBuf[3] = TTemp;
    TransmitBytes(32);  //发送同步信号
    delay(500);
    j ++;
}
```

节点程序为从机如果接收到主机的同步信号（帧头为0xdd的信号），就把自己定时器的值与各状态计数器的值进行修正。

节点程序以下：

```
if((Recepacket(20,32) == 1)&&(RxBuf[0] == 0xdd))//接收同步信号;
    {
        ……          //清除各种标志位
        TR0 = 0;
        TH0 = RxBuf[1];
        TL0 = RxBuf[2];
        TR0 = 1;
        TTemp = RxBuf[3];
        TBFlag = 1;          //修正同步时间
    }
```

3.3.3.2 广播信号时段

首先介绍一个重要的结构体，此结构体为网络在传送数据的帧格式，包括帧头、地址、帧长度、数据、加和校验、帧尾。

主机程序为主机向节点发送广播或向单一节点发送数据的程序。

已经讲了在广播时段的数据结构，这里定义广播数据的帧头为0xff，所有广播或主机向单一节点发送的数据都采用这个帧头。

由于实验时串口进来的地址数据用的是ASCII码，所以在程序中，地址处理需要多次用到数据转换。这个网络最多支持32个节点，而地址位只有一个字节，因此需要把数字大于10的地址用大写字母表示，地址用0～9和A～W来表示，其中A～W分别表示10～32。

因为射频模块每次只能传送32个字节的数据，除去帧头、帧尾、数据长度、地址、加和校验位之后，其实一帧数据的长度只有32－5＝27字节。所以数据大于27字节以上的都只能分成几次传送。另外在传送过程中，帧尾表示的是现在传送的是第几帧数据，如果为第一帧，则帧尾就为0x01；如果是最后一帧或只有一帧数据，帧尾都为0xff。

每一帧数据都做了一个加和校验，这样可以保证数据的正确性，如果节点收到的数据不通过加和校验，证明数据传送错误，节点会自动丢弃数据。

如果主机发送广播信号就不需要接收节点的应答信号，如果是向单一节点发送数据就需要接收节点的应答信号，以确认该节点已经正确地收到数据。同时主机无论有没有收到单一节点的应答信号，都会从串口发出发送数据成功与否的信号。这里，当数据发送成功后，主机串口返回 “@” + “Y” + “节点地址（单字节）” + “ * ”。如果发送不成功，串口返回：“@” + “N” + “节点地址（单字节）” + “ * ”。所以可以通过串口看出发送数据成功与否。

当要发送广播或发送数据给单一节点时，如果从串口发送命令，发送地址为 0 时表示广播信号，发送地址为其他数据时为发给单一节点的数据，这一点会在以后的试验部分介绍。

节点程序为节点接收广播的程序，首先判断是广播信号（帧头是否为 0xff），且与自己的地址匹配，就把收到的数据存入 BroadCast 数据缓冲区里面。如果接收完成且加和校验能通过，证明接收正确，就把收到的广播数据或主机发给自己的数据全部从串口输出。此时如果是广播信号就不用发送应答信号，如果是单一发给自己的数据就要发送应答信号，通知主机数据接收正确。

3.3.3.3 加入退出网络时段

主机部分首先说明几个重要的全局变量：

```
INT8U AddrRam [32]。          //存储在线终端 ID 号用
INT8U AddrPoint = 0。         //现在在线终端的个数
/ * AddrRam [32]：是用来存储在线终端的 ID 用的，如果有新的节点加入，就把该节点的 ID 号存入该数组，同样，如果有节点想要退出网络，就把该节点的 ID 号从数组中删除。这里最多只能存储 32 个 ID 号。 * /
```

由于接收程序有超时计数器，这里主机程序（见下面主机程序）进行了 9 次接收，所以如果每次都有节点加入的话，最多一起只能加入 9 个节点。

在这里定义加入网络信号的帧头为：0xee，退出网络信号的帧头为：0xe0。

可以当成主机在这个时段一直处于接收状态，如果收到加入网络信号，就把该节点的节点号存入存储网络 ID 号的缓冲区里（AddrRam），同时使网络中的节点数 AddrPoint 加 1，然后发送应答信号，通知节点已经加入了网络。反之，如果有节点想要退出网络也一样，主机首先在存储 ID 号的缓冲区里找到要退出网络的 ID 号，然后再把该 ID 号删除，同时使网络中的节点数 AddrPoint 减 1，然后发送应答信号，通知节点已经退出了网络。

如果有节点加入或退出网络，主机都会把该信号从串口输出。如果有节点加入网络，串口输出： “@” + “E” + “节点号（单字节）” + “ * ”。如果有节点退出网络：“@” + “E” + “节点号（单字节）” + “ * ”。

主机程序以下：

```
//******************************************************************************
//函数名:void OpenJionNet(void)
//输入:无
//输出:无
//功能描述:加入网络时段
```

```
//************************************************************************
void OpenJionNet(void)
{
    INT8U i =0;
    while(i <9)
    {
        memset(RxBuf,0,32);
        if(Recepacket(10,32) ==1)
        {
            if((RxBuf[0] ==0xee)&&(RxBuf[31] ==0xff))//如果是加入网络信号
            {
                AddrRam[AddrPoint] = RxBuf[1];  //存入缓冲区
                AddrPoint ++;                   //地址指针加一,指向栈顶空位
                NetKeepCount[RxBuf[1]] =0;        //刚加入时网络维持计数器清零
                TxBuf[0] =0xee;
                TxBuf[1] = RxBuf[1];
                TxBuf[31] =0xff;
                TransmitBytes(32);                  //发送应答信号
                SendCh('@');
                SendCh('E');                    //有节点加入
                SendCh(RxBuf[1] >9? (RxBuf[1] +0x37):(RxBuf[1] +0x30));
                SendCh('*');
            }
            if((RxBuf[0] ==0xe0)&&(RxBuf[31] ==0xff))
            {
                i =0;
                while((i < AddrPoint)&&(AddrRam[i] ! =RxBuf[1]))
                {
                    i ++;
                }
                if(i < AddrPoint)
                {
                    AddrRam[i] = AddrRam[AddrPoint-1];          //栈顶的ID号移到此位
                    AddrRam[AddrPoint-1] =0;                    //最顶上的ID清零
                    AddrPoint- =1;                                //地址指针减一
                    TxBuf[0] =0xe0;
                    TxBuf[1] = RxBuf[1];
                    TxBuf[31] =0xff;
                    TransmitBytes(32);                            //发送应答
                    SendCh('@');
                    SendCh('O');                                //有节点退出
                    SendCh(RxBuf[1] >9? (RxBuf[1] +0x37):(RxBuf[1] +0x30));
                    SendCh('*');
```

```
            }
            else
            {
                ;
            }
        }
    }
    i++;
  }
}
```

节点加入和退出网络的程序结构都一样，节点首先产生一个0~7ms的随机延时，这样如果几个节点一起加入网络，随机延时函数算得比较快的节点就会首先发送加入网络信号。然后节点进入接收状态，判断现在信道是否为空，如果随机延时函数算得比较快的节点在与主机通信，这时模块的DR信号就会为高，这时其他节点是不能与主机通信的，所以其他节点只能再进行一次随机延时，再检测信道是否为空，如此直到信道为空时才能与主机通信从而加入网络。如果连续三次节点都检测到信道被占用，节点就退出加入网络状态，等下一个加入网络时段再加入或退出网络。节点发送加入退出网络后，如果收到了来自主机带ID号的应答信号后，如果ID号与自己的相同，则加入退出网络成功。

3.3.3.4 网络维持及数据交换申请时段

A 全局变量说明

首先说明几个全局变量如下：

```
INT8U AddrRam[32];      //存储在线终端地址用
INT8U AddrPoint = 0;    //现在在线终端的个数
INT8U NetKeepflag[32];  //网络维持标志位
INT8U NetKeepCount[32]; //网络维持计数器,连续三次不在,认为该节点退出
```

AddrRam[32]和AddrPoint上一节已经说明过了，这里就不多作说明了。

(1) NetKeepflag：网络维持标志位，因为主机在每个网络维持时段都会检测一次所有的节点在不在网络中，如果节点在网络中，就会主动和主机通信一次，这时这个网络维持标志位就会置为“1”，表示它在网络中，所以看出NetKeepflag是用于统计节点在不在网络中用的。

(2) NetKeepCount[32]：是和NetKeepflag[32]一起用作统计节点在不在网络中用的。NetKeepCount[32]是一个计数器，主机每次都在网络维持及数据交换申请时段统计一次节点在不在网络中，如果节点不在网络中，该节点的计数器就会加1，当主机统计节点三次不在网络中时，主机就认为节点已经脱离了网络。

B 主机程序说明

主机在这个时段内一直处于接收状态，如果收到网络维持信号或申请数据交换信号后，主机会自动给予应答。并把该节点存在网络中的标志位置为“1”。

(1) INIT_905(3)：这个函数是配置NRF905每次只能发送或接收三个字节，这样

做是为了节省发送和接收的时间。由于 NRF905 的传输速度最大只能达到 100kb/s，相当于十多 K 字节每秒，为了提高整个网络的实时性，所以用这个方法提高通信效率，等到这个时段过了之后，在下一个时段有大量数据要交换的时候就把它配置回每次发送 32 个字节。

（2）ResetTimer（2）：为复位软件定时器 2

（3）while（ReadTimer（2）<450）：这是一个超计数定时器，软件定时器 2 复位以后，在计时器小于一定时间内，主机都处于接收状态，直到超时退出。

每次当主机接收到节点的网络维持信号或数据申请交换信号后（节点如果有数据申请交换，证明节点还在网络中，就不必在这个周期中发送网络维持信号了），就会把相应的节点网络标志位置 1，同时把 NetKeepCount[32] 计数器清零，然后向节点发送应答信号。

另外说明一下，主机会在主程序里在这个时段最后阶段统计网络中所有节点有没有发送网络维持信号或发送数据申请交换信号，即网络中的标志位是否置 1，如果连续三次都没有发送网络维持信号，则证明节点已经不在网络中了。

```
//********************************************************************
//函数名:void NetDataSwitch(void)
//输入:无
//输出:无
//功能描述:数据交换申请及网络维护时段
//********************************************************************
void NetDataSwitch(void)
{
    INT8U Sender = 0;
    INT8U kk;
    INIT_905(3);
    memset(DataIDBuf,0,32);
    DataIDPoint = 0;
    ResetTimer(2);
    while(ReadTimer(2) <450)
    {
      if(Recepacket(10,3))
      {
        if(RxBuf[0] ==0x88)
        {
          Sender = RxBuf[1];
          DataIDBuf[DataIDPoint] = Sender;
          DataIDPoint ++;
          kk =0;
          while((kk < = AddrPoint)&&(AddrRam[kk]! = Sender))
          {
              kk ++;
```

```
        }
        if(kk < = AddrPoint)
      //此节点是在网络里的节点,有数据发相当于发送一次网络维护信号
        {
            NetKeepflag[AddrRam[kk]] = 1;//节点存在的标志位置1
            NetKeepCount[AddrRam[kk]] = 0;
        }
        TxBuf[0] = 'Y';
        TxBuf[1] = Sender;
        TransmitBytes(3);
      }
      if(RxBuf[0] == 0xB0)
      {
        Sender = RxBuf[1];
        kk = 0;
        while((kk < = AddrPoint)&&(AddrRam[kk]! = Sender))
        {
            kk ++;
        }
        if(kk < = AddrPoint)          //此节点是在网络里的节点,就发送应答信号
        {
            NetKeepflag[AddrRam[kk]] = 1;//节点存在的标志位置1
            NetKeepCount[AddrRam[kk]] = 0;
            TxBuf[0] = 'Y';
            TxBuf[1] = Sender;           //发送应答信号
            TransmitBytes(3);
        }
      }
    }
  }
  INIT_905(32);
}
```

节点分为发送网络维持信号和申请数据交换信号。

C 节点程序说明

INIT_905(3)程序和主机一样，先把发送和接收函数配置成一次只能发送接收三个字节的函数。

if(ReadTimer(2) == ID * 5)：这时采用时分的方式向主机发送网络维持信号，为了避免信号在空中相撞。这样每一个在网络中的节点都有自己的ID号，所以各自发送信号的时间也各不相同。每个节点在这个时段都会与主机自动通信一次，但是又为能同时与主机通信，所以只能一个一个与主机通信。用时分的方法是在这个小的网络里最有效、最简单的通信方法。

上面两个函数可以看出，我们网络中表示数据申请交换帧的帧头为0x88，而表示网络维持信号的帧头为0xB0。

两个函数都是收到主机的应答信号就表示发送成功，否则失败。然后再把发送接收的字节数配置回每次32个字节。

3.3.3.5 点对点数据交换时段

A 主机程序说明

主机在这个时段依次访问在数据申请交换时段时申请了有数据交换的节点。然后把节点发送回来的数据以“@” + “节点ID号（单字节）” + “数据” + “*”。的格式通过串口发送出来。流程图如图3-59所示。

程序中可以看出，我们设定了一个Time-Temp变量，是为了保证与一个节点交换数据的时间不要太长，不然后面的节点就没有机会在这个时段与主机交换数据了。因为我们这个系统只适合传送不超时100字节的数据，所以我们在这里设定了100ms的超时，在这个时间内应该可以完成所有数据的交换，不然就应该以出错处理，开始和下一个节点交换数据。

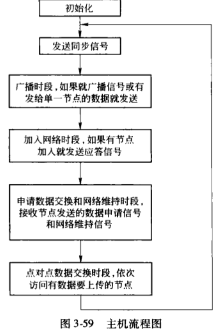


图3-59 主机流程图

主机依次访问节点索取数据的帧头为0x80。

主机在这个时段首先判断有无节点需要交换数据，如果有就开始打包发送索取数据信号，DataIDBuf[i]有数据要发送给主机的ID号地址，主机会依次数组里面的节点。如果此时节点收到索取数据信号，就开始向主机发送数据。主机接收数据的时候，同时进行加和校验验证，如果校验不能通过，就退出这次数据交换。当收到最后一包数据时（最后一包数据的最后一个帧尾为0xff)，且主机校验通过后，主机向该节点发送应答信号，然后开始下一个节点的数据交换。

B 节点程序说明

有数据想要交换的节点在点对点数据交换时段会一直处在接收状态，因为在数据申请交换时段已经跟主机发送了申请信号。所以在这个时段如果收到主机的索取数据信号后，确认ID号匹配后，节点开始发送自己的数据，直到数据发送完成后收到主机的确认应答信号。

节点发送数据的格式为：

帧头（0x88）	地址（本机ID号）	数据长度	数据	加和校验位	帧尾（第几帧数据）

程序在发送数据的时候，是一帧一帧发送的，因为我们现在无线发送一帧数据最多只能发送32字节，除去帧头、帧尾、数据长度、地址、加和校验位之后，其实我们一帧数

据的长度只有 32 - 5 = 27 字节，所以当数据大于 27 字节的时候都只有分成几次传送。数据长度是指这一帧里有效数据的个数，即除去帧头、帧尾、数据长度、地址、加和校验位之外的数据。另外在我们传送程序过程中，帧尾表示的是现在传送的是第几帧数据，如果为第一帧，则帧尾就为 0x01；如果是最后一帧或一共只有一帧数据，帧尾都为 0xff。

C 主机源代码及说明

主机程序首先是初始化程序，初始化 CPU、定时器、串口、NRF905，之后程序进入主循环程序，循环执行五个时段的程序。

两个 LED 可以指示四种状态，我们让广播时段和加入网络时段共用一种指示。所以可以从两个 LED 的状态看出现在在哪个时段。

（1）同步时段：主机一到同步时段就马上打包发送同步信号，为了让所有节点有效收到同步信号，主机连续发送三次同步信号。

（2）广播时段：如果主机从串口收到需要广播的数据或是发送给单一节点的数据，主机就在这个时段发送广播信号或者单一发给一个节点数据。

（3）加入退出网络时段：主机在这个时段一旦处于接收状态，一旦接收到加入退出网络的信号就指导该节点的 ID 号存入缓冲区里，并发送应答信号。

（4）数据申请交换和网络维持时段：主机在这个时段一开始的大部分时间都处于接收状态，接收节点的数据申请交换和网络维持信号，一旦网络中的节点有发送数据申请交换和网络维持就把相应的节点网络标志位置 1，同时把 NetKeepCount[32]计数器清零，然后向节点发送应答信号。如果是发送的数据申请交换信号，就把该节点的 ID 号存入 DataIDBuf 数组里，以便在点对点数据交换时段向该节点索取数据。然后主机会在最后时段统计网络中所有节点有没有发送网络维持信号或发送数据申请交换信号，即网络中的标志位是否置 1，如果连续三次都没有发送网络维持信号，则证明节点已经不在网络中了。即从串口发出“@” + “O” + “节点 ID 号” + “ * ”，然后把该节点从 AddrRam 数组中删除，同时使网络中节点数 AddrPoint 减 1。

（5）点对点数据交换时段：如果在上一个时段，有节点发送了数据申请交换信号，主机在该时段就会依次访问发送了数据申请交换信号的节点。并把节点发送过来的数据从串口发出。

节点主程序首先也是进行初始化程序和清除各种标志位。流程图如图 3-60 所示。

然后程序进入主循环程序，同样循环执行五个时段。两个 LED 的显示也跟主机的同步。

（1）同步时段：节点在此时处于接收状态，接收主机发送的同步信号，如果接收到主机的同步信号，就修正自己的定时计数器，使时间与主机同步。节点在同步时段只接收一次主机发送的同步信号。如果主机在这个时段没有收到主机发送的同步信号，节点不会进入下一个时段，而是一直在接收主机的同步信号，直到收到同步信号为止。

（2）广播时段：如果节点已经加入网络，节点就可以在这个时段接收主机发送的广播信号。

（3）加入网络时段：如果节点还没有加入网络，节点会在这个时段发送加入网络信号，如果加入网络成功，节点会把自己在网络中的标志位置 1，表示自己已经加入网络，下一个加入网络时段就不会发送加入网络信号了。

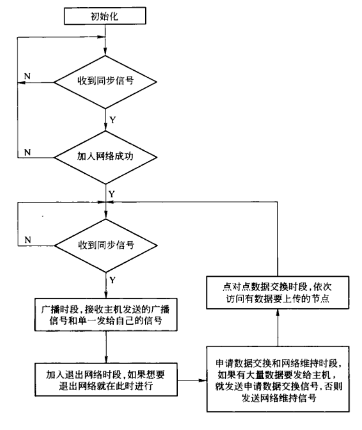


图3-60 节点主程序流程图

（4）数据申请交换和网络维持时段：节点首先判断有没有从串口收到要发送给主机的数据，如果有，节点就发送数据申请交换信号，如果没有，就发网络维持信号。如果发送数据申请交换信号成功，就把数据申请交换标志位置1。如果三次发送网络维持信号都不成功，就认为自己已经退出了网络。节点马上停止工作，并从串口发出节点已经退出网络信息“Out_Net”。

（5）点对点数据交换时段：如果节点有数据要发送给主机，且节点在上一个时段已经发送数据申请交换信号成功，且数据申请交换标志位已经置1。节点在这个时段就处于接收状态，接收主机发送的索取数据信号，如果地址与自己的地址匹配，就开始发送自己的数据。同时清除串口有新数据标志位。

3.4 主要无线传感网技术和国际标准

怎样不通过电缆，摆脱物理连接上的限制，使设备互联起来呢？为了找到这个问题的答案，十多年来，人们不断探索，形成了当今令人眼花缭乱的无线通信协议和产品。

随着数字通信和计算机技术的发展，许多无线通信的要求被提出，短距离无线通信和长距离无线通信有很多方面的区别，主要的特征如下：

(1) 无线发射功率在几微瓦到小于 100 微瓦；
(2) 通信距离范围在几厘米到几百米；
(3) 主要在房间内使用；
(4) 使用全向天线和线路板天线；
(5) 不需要申请无线频道；
(6) 高频操作；
(7) 电池供电的无线发射器和无线接收器。

典型的短距离无线系统由一个无线发射器（包括数据源、调制器、RF 源、RF 功率放大器、天线、电源组成）和一个无线接收器（包括数据接收电路、RF 解调器、译码器、RF 低噪声放大器、天线、电源）组成。

随着无线的发展，网络化、标准化要求逐渐出现在人们的面前。因此各种无线网络技术标准纷纷被制订出来。以下我们来看看目前比较热门的几种无线网络技术标准。根据不同的应用要求，多种无线网络技术被应用到无线传感网中。

无线网络是利用无线电射频（Radio Frequency，RF）或红外线（Infrared，IR）等无线传输媒体与技术构成的通信网络系统。由于取消了有线介质（双绞线、同轴电缆、光纤等），使得网络用户真正达到"信息随身化、便利走天下"的理想境界。

目前五种短距离无线网络技术正在成为业界谈论的焦点，它们分别是 ZigBee、无线局域网（Wi-Fi）、蓝牙（Bluetooth）、超宽频（Ultra Wide Band）和近距离无线传输（NFC）。

3.4.1 IEEE802.15.4/ZigBee 无线网络技术

ZigBee 是一种新兴的短距离、低速率无线网络技术，它是一种介于无线标记技术和蓝牙之间的技术提案。它此前被称作"HomeRF Lite"或"FireFly"无线技术，主要用于近距离无线连接。它有自己的无线电标准，在数千个微小的传感器之间相互协调实现通信。这些传感器只需要很少的能量，以接力的方式通过无线电波将数据从一个传感器传到另一个传感器，所以它们的通信效率非常高。最后，这些数据就可以进入计算机用于分析或者被另外一种无线技术如 WiMax 收集。

ZigBee 的基础是 IEEE802.15.4，这是 IEEE 无线个人区域网（Personal Area Network，PAN）工作组的一项标准，被称作 IEEE802.15.4（ZigBee）技术标准。

ZigBee 不仅只是 802.15.4 的名字。IEEE 仅处理低级 MAC 层和物理层协议，因此 ZigBee 联盟对其网络层协议和 API 进行了标准化。完全协议用于一次可直接连接到一个设备的基本节点的 4K 字节或者作为 Hub 或路由器的协调器的 32K 字节。每个协调器可连接多达 255 个节点，而几个协调器则可形成一个网络，对路由传输的数目则没有限制。ZigBee 联盟还开发了安全层，以保证这种便携设备不会意外泄漏其标识，而且这种利用网络的远距离传输不会被其他节点获得。

ZigBee 联盟成立于 2001 年 8 月。2002 年下半年，英国 Invensys 公司、日本三菱电气公司、美国摩托罗拉公司以及荷兰飞利浦半导体公司四大巨头共同宣布，它们将加盟"ZigBee 联盟"，以研发名为"ZigBee"的下一代无线通信标准，这一事件成为该项技术发展过程中的里程碑。

到目前为止，除了 Invensys、三菱电子、摩托罗拉和飞利浦等国际知名的大公司外，该联盟已有 200 多家成员企业，并在迅速发展壮大。其中涵盖了半导体生产商、IP 服务提供商、消费类电子厂商及 OEM 商等，例如 Honeywell、Eaton 和 Invensys Metering Systems 等工业控制和家用自动化公司，甚至还有像 Mattel 之类的玩具公司。所有这些公司都参加了负责开发 ZigBee 物理和媒体控制层技术标准的 IEEE802.15.4 工作组。

相对于常见的无线通信标准，ZigBee 协议栈紧凑简单，具体实现要求很低。只要 8 位处理器再配上 4kB ROM 和 64kB RAM 等，就可以满足其最低需要，从而大大降低了芯片的成本。完整的 ZigBee 协议栈模型如图 3-61 所示。

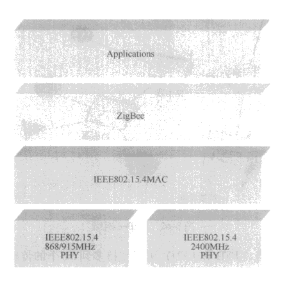


图 3-61　ZigBee 协议栈结构图

ZigBee 协议栈由高层应用规范、应用汇聚层、网络层、数据链路层和物理层组成，网络层以上的协议由 ZigBee 联盟负责，IEEE 则制定物理层和链路层标准。应用汇聚层把不同的应用映射到 ZigBee 网络上，主要包括安全属性设置和多个业务数据流的汇聚等功能。网络层将采用基于 Ad Hoc 技术的路由协议，除了包含通用的网络层功能外，还应该与底层的 IEEE802.15.4 标准同样省电。另外，还应实现网络的自组织和自维护，以最大限度地方便消费者使用，降低网络的维护成本。

ZigBee 是一个由可多到 65000 个无线数传模块组成的无线数传网络平台，十分类似现有的移动通信的 CDMA 网或 GSM 网，每一个 ZigBee 网络数传模块类似移动网络的一个基站，在整个网络范围内，它们之间可以进行相互通信；每个网络节点间的距离可以从标准的 75 米，到扩展后的几百米，甚至几公里；另外整个 ZigBee 网络还可以与现有的其他的各种网络连接。例如，你可以通过互联网在北京监控云南某地的一个 ZigBee 控制网络。

不同的是 ZigBee 网络主要是为自动化控制数据传输而建立，而移动通信网主要是为语音通信而建立；每个移动基站价值一般都在百万元人民币以上，而每个 ZigBee "基站"却不到 1000 元人民币；每个 ZigBee 网络节点不仅本身可以与监控对象例如传感器连接直接进行数据采集和监控，还可以自动中转别的网络节点传过来的数据资料；除此之外，每一

个 ZigBee 网络节点（FFD）还可在自己信号覆盖的范围内和多个不承担网络信息中转任务的孤立的子节点（RFD）无线连接，如图 3-62 所示。

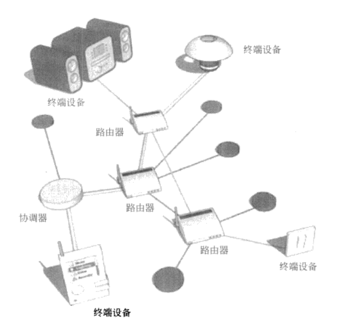


图 3-62　ZigBee 网络

每个 ZigBee 网络节点（FFD 和 RFD）可以支持多到 31 个的传感器和受控设备，每一个传感器和受控设备可以有 8 种不同的接口方式。可以采集和传输数字量和模拟量。

ZigBee 技术的特点包括以下几方面：

（1）省电。两节五号电池支持长达 6 个月到 2 年左右的使用时间。

（2）可靠。采用了碰撞避免机制，同时为需要固定带宽的通信业务预留了专用时隙，避免了发送数据时的竞争和冲突；节点模块之间具有自动动态组网的功能，信息在整个 ZigBee 网络中通过自动路由的方式进行传输，从而保证了信息传输的可靠性。

（3）时延短。针对时延敏感的应用做了优化，通信时延和从休眠状态激活的时延都非常短。

（4）网络容量大。可支持达 65000 个节点。

（5）安全。ZigBee 提供了数据完整性检查和鉴权功能，加密算法采用通用的 AES-128。

（6）高保密性。64 位出厂编号，支持 AES-128 加密。

详细 ZigBee 介绍请查阅冶金工业出版社出版的《ZigBee 无线网络原理》。在《ZigBee 无线网络原理》中将为读者详细分析 ZigBee 协议栈以及相关原理。

ZigBee 技术和 RFID 技术在 2009 年就被列为当今世界发展最快，市场前景最广阔的十大最新技术中的两个。关于这方面的报道，只需在百度或 Google 搜索栏中键入“ZigBee”，就能看到大量的相关信息。总之，今后若干年，都将是 ZigBee 技术飞速发展的时期。

尽管，国内不少人已经开始关注 ZigBee 这门新技术，而且也有不少单位开始涉足 ZigBee 技术的开发工作，然而，由于 ZigBee 本身是一种新的系统集成技术，应用软件的开发必须和网络传输、射频技术和底层软硬件控制技术结合在一起。因而深入理解这个来自国外的新技术，再组织一个在这几个方面都有丰富经验的配套的队伍，本身就不是一件容易的事情。因而到目前为止，国内有关 ZigBee 开发的公司还是很少。但可喜的是目前一些高校以及公司相继加入到了 ZigBee 的开发行列中。

3.4.2 IEEE802.11/Wi-Fi 无线网络技术

Wi-Fi 为 IEEE 定义的一个无线网络通信的工业标准（IEEE802.11）。Wi-Fi 第一个版本发表于 1997 年，其中定义了介质访问接入控制层（MAC 层）和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式，总数据传输速率设计为 2Mb/s。两个设备之间的通信可以自由直接（Ad hoc）的方式进行，也可以在基站（Base Station，BS）或者访问点（Access Point，AP）的协调下进行。

一个 Wi-Fi 连接点，网络成员和结构，站点（Station）是网络最基本的组成部分。

（1）基本服务单元（Basic Service Set，BSS）。网络最基本的服务单元。最简单的服务单元可以只由两个站点组成。站点可以动态地连接（associate）到基本服务单元中。

（2）分配系统（Distribution System，DS）。分配系统用于连接不同的基本服务单元。分配系统使用的媒介（Medium），逻辑上和基本服务单元使用的媒介是截然分开的，尽管它们物理上可能会是同一个媒介，例如同一个无线频段。

（3）接入点（Access Point，AP）。接入点即有普通站点身份，又有接入到分配系统（DS）的功能。

（4）扩展服务单元（Extended Service Set，ESS）。由分配系统和基本服务单元组合而成。这种组合是逻辑上，并非物理上的——不同的基本服务单元物有可能在地理位置相去甚远。分配系统也可以使用各种各样的技术。

（5）关口（Portal）。也是一个逻辑成分、用于将无线局域网和有线局域网或其他网络联系起来。

站点使用的无线的媒介、分配系统使用的媒介以及和无线局域网集成一起的其他局域网使用的媒介。在物理上可能互相重叠。IEEE802.11 只负责在站点使用的无线的媒介上的寻址（Addressing）。分配系统和其他局域网的寻址不属无线局域网的范围。

IEEE802.11 没有具体定义分配系统，只是定义了分配系统应该提供的服务（Service）。整个无线局域网定义了 9 种服务：5 种服务属于分配系统的任务，分别为连接（Association）、结束连接（Diassociation）、分配（Distribution）、集成（Integration）、再连接（Resuscitation）。4 种服务属于站点的任务，分别为鉴权（Authentication）、结束鉴权（Deauthentication）、隐私（Privacy）、MAC 数据传输（MSDU delivery）。

1999 年加上了两个补充版本 802.11a 定义了一个在 5GHz ISM 频段上的数据传输速率可达 54Mb/s 的物理层，802.11b 定义了一个在 2.4GHz 的 ISM 频段上但数据传输速率高达 11Mb/s 的物理层。2.4GHz 的 ISM 频段为世界上绝大多数国家通用，因此 802.11b 得到了最为广泛的应用。苹果公司把自己开发的 802.11 标准起名叫 AirPort。

1999 年工业界成立了 Wi-Fi 联盟，致力解决符合 802.11 标准的产品的生产和设备兼

容性问题。

（1）802.11 的标准和版本。1997 年 802.11 原始标准（2Mb/s，工作在 2.4GHz）。

（2）802.11a，1999 年，物理层补充（54Mb/s 工作在 5GHz）。1999 年 802.11b 物理层补充（11Mb/s，工作在 2.4GHz）。

（3）802.11c 符合 802.1D 的媒体接入控制层（MAC）桥接（MAC Layer Bridging）。

（4）802.11d，根据各国无线电规定做的调整。

（5）802.11e 对服务等级（Quality of Service，QS）的支持。

（6）802.11f 基站的互连性（Interoperability）。

（7）802.11g，物理层补充（54Mb/s，工作在 2.4GHz）。802.11h，无线覆盖半径的调整，室内（indoor）和室外（outdoor）信道（5GHz 频段）。

（8）802.11i，安全和鉴权（Authentification）方面的补充。

（9）802.11n，导入多重输入输出（MIMO）技术，基本上是 802.11a 的延伸版。

除了上面的 IEEE 标准，另外有一个被称为 IEEE802.11b + 的技术，通过 PBCC 技术（Packet Binary Convolutional Code）在 IEEE802.11b（2.4GHz 频段）基础上提供22Mb/s 的数据传输速率。但这事实上并不是一个 IEEE 的公开标准，而是一项产权私有的技术（产权属于美国得州仪器，Texas Instruments）。也有一些被称为 802.11g + 的技术，在 IEEE802.11g 的基础上提供 108Mb/s 的传输速率，跟 802.11b + 一样，同样是非标准技术，由无线网络芯片生产商 Atheros 所提倡的则为 SuperG。

Wi-Fi（wireless fidelity 无线保真）实质上是一种商业认证，具有 Wi-Fi 认证的产品符合 IEEE802.11b 无线网络规范，它是当前应用最为广泛的 WLAN 标准，采用波段是 2.4GHz。IEEE802.11b 无线网络规范是 IEEE802.11 网络规范的变种，最高带宽为 11Mb/s，在信号较弱或有干扰的情况下，带宽可调整为 5.5Mb/s、2Mb/s 和 1Mb/s，带宽的自动调整，有效地保障了网络的稳定性和可靠性。

自从实行 IEEE802.11b 以来，无线网络取得了长足的进步，因此基于此技术的产品也逐渐多了起来，解决各厂商产品之间的兼容性问题就显得非常必要。因为 IEEE 并不负责测试 IEEE802.11b 无线产品的兼容性，所以这项工作就由厂商自发组成的非营利性组织——Wi-Fi 联盟来担任。这个联盟包括了最主要的无线局域网设备生产商，如 Intel、Broadcom，以及大家熟悉的中国厂商华硕、BenQ 等。凡是通过 Wi-Fi 联盟兼容性测试的产品，都被准予打上"Wi-Fi CERTIFIED"标记。因此，我们在选购 IEEE802.11b 无线产品时，最好选购有 Wi-Fi 标记的产品，以保证产品之间的兼容性。

Wi-Fi 技术突出的优势在于如下几个方面：

（1）无线电波的覆盖范围广。基于蓝牙技术的电波覆盖范围非常小，半径大约只有 50 英尺左右约合 15 米，而 Wi-Fi 的半径则可达 300 英尺左右约合 100 米，办公室自不用说，就是在整栋大楼中也可使用。最近，Vivato 公司推出了一款新型交换机。据悉，该款产品能够把目前 Wi-Fi 无线网络 300 英尺接近 100 米的通信距离扩大到 4 英里约 6.5 公里。

（2）虽然由 Wi-Fi 技术传输的无线通信质量不是很好，数据安全性能比蓝牙差一些，传输质量也有待改进，但传输速度非常快，可以达到 11Mb/s，符合个人和社会信息化的需求。

（3）厂商进入该领域的门槛比较低。厂商只要在机场、车站、咖啡店、图书馆等人员

较密集的地方设置"热点"，并通过高速线路将因特网接入上述场所。这样由于"热点"所发射出的电波可以达到距接入点半径数十米至100米的地方，用户只要将支持无线LAN的笔记本电脑或PDA拿到该区域内，即可高速接入因特网。也就是说，厂商不用耗费资金来进行网络布线接入，从而节省了大量的成本。

Wi-Fi的主要特点是传输速率高、可靠性高、建网快速、便捷、可移动性好、网络结构弹性化、组网灵活、组网价格较低等，因此具有良好的发展前景。

IEEE802.11规范是在1997年8月提出的，规定了3种物理层介质，即红外线、光波和ISM 2.4～2.4835GHz频段的无线电波。其中后者采用了两种扩频技术DSSS和FHSS。但是由于这个标准只能提供1～2Mb/s的速率，远远低于当时有线以太网普遍提供的10Mb/s的速率，所以没有引起足够的重视。

IEEE802.11b发布于1999年9月。与IEEE802.11不同，它只采用2.4GHz的ISM频段的无线电波，且采用加强版的DSSS，它可以根据环境的变化在11Mb/s、5.5Mb/s、2Mb/s和1Mb/s之间动态切换，目前802.11b协议是当前最为广泛的WLAN标准。其缺点是速率还是不够高，且所在的2.4GHz的ISM频段的带宽比较窄（仅有85MHz），同时还要受微波、蓝牙等多种干扰源的干扰。

3.4.3 IEEE802.15.1/蓝牙无线网络技术

蓝牙（Bluetooth）是1994年由爱立信公司首先提出的一种短距离无线通信技术规范，这个技术规范是使用无线连接来替代已经广泛使用的有线连接。1999年12月1日，蓝牙特殊利益集团发布了"蓝牙"标准的最新版1.0B版。该最新版"蓝牙"标准主要定义的是底层协议，同时为保证和其他协议的兼容性，也定义了一些高层协议和相关接口。

"蓝牙"标准的协议栈中的高层协议包括：串口通信协议（RFCOMM），电话控制协议（TCS）、对象交换协议（OBBX）、控制命令（ATCommand）、vGard和vCalender电子商务表中协议、PPP、IP、TCP、UDP等与因特网相关的协议以及WAP协议。就其工业实现而言，"蓝牙"标准可以分为硬件和软件两个部分，硬件部分包括射频/无线电协议、基带/链路控制器协议和链路管理器协议，一般是做成一个芯片。软件部分则包括逻辑链路控制与适配协议及其以上的所有部分。硬件和软件之间通过HCI进行连接，也就是说HCI在硬件和软件中都有，两者提供相同接口进行通信。

蓝牙（Bluetooth）作为一种小范围无线连接技术，能够在设备间实现方便快捷、灵活安全、低成本、低功耗的数据和语音通信，是目前实现无线个域网的主流技术之一。同时，蓝牙系统以Ad hoc的方式工作，每个蓝牙设备都可以在网络中实现路由选择的功能，可以形成移动自组织网络。蓝牙的特性在许多方面正好符合Ad hoc和WPAN的概念，显示其真正的潜力所在。而且，将蓝牙与其他网络相连接可带来更广泛的应用，例如接入Internet、PSTN或公众移动通信网，可以使用户应用更方便或给用户带来更大的实惠。

蓝牙技术是一种尖端的开放式无线通信标准，能够在短距离范围内无线连接台式电脑与笔记本电脑、便携设备、PDA、移动电话、拍照手机、打印机、数码相机、耳麦、键盘甚至是电脑鼠标。蓝牙无线技术使用了全球通用的频带（2.4GHz），以确保能在世界各地通行无阻。简言之，蓝牙技术让各种数码设备之间能够无线沟通，让散落各种连线的桌面

成为历史。

蓝牙技术的应用范围相当广泛，目前已经进入到了许多主流消费性产品当中，比如在手机、PDA、笔记本电脑等方面应用。台式电脑基本都没有现成的蓝牙通信口，如果要实现手机等具备蓝牙功能的设备和电脑实现无线蓝牙通信，需要在电脑端配备蓝牙适配器使其具有蓝牙通信功能，从而实现蓝牙无线通信。

蓝牙无线通信技术在欧美是一种比较成熟的技术，广泛应用于生活领域中。其工作频段是一个不受限制的自由频段，采用跳频工作方式和先进的加密技术，使蓝牙在传输文件时具有较高的安全性。使用时进行匹配，而后即可通过蓝牙手机进行数据交换，在电脑中实现网页浏览。

蓝牙是无线网络传输技术的一种，原本是用来取代红外的。与红外技术相比，蓝牙无需对准就能传输数据，传输距离小于 10m（红外的传输距离在几米以内）。而在信号放大器的帮助下，通信距离甚至可达几十米左右。蓝牙系统一般由无线单元、链路控制（固件）单元、链路管理（软件）单元和蓝牙软件（协议栈）单元等 4 个功能单元组成。无线单元射频部分通过 2.4GHz ISM 频段的微波来实现数据位流的过滤和传输。蓝牙要求其天线部分体积十分小巧、重量轻。因此，蓝牙天线属于微型天线。

蓝牙系统主要有以下特点：

（1）工作在 2.4GHz 的 ISM 频段，工作频段无需申请许可；

（2）当发射功率为 1mW 时，通信距离可以达到 10m，发射功率为 100mW 时，通信距离不到 100m；

（3）使用 1Mb/s 速率以达到最大限制带宽；

（4）使用快速调频（1600 跳/s）技术抗干扰；

（5）在干扰下，使用短数据帧尽可能增大容量；

（6）快速确认机制能在链路情况良好时实现较低的编码开销；

（7）采用 CVSD 语音编码，可在高误码率下使用；

（8）灵活帧方式支持广泛的应用领域；

（9）宽松链路配置支持低价单芯片集成；

（10）严格设计的空中接口使功耗最小；

（11）发射功率自适应，低干扰；

（12）采用灵活的无基站组网方式，使得一个“蓝牙”单元最多同时可以和 7 个其他的“蓝牙”单元通信，同时支持点对点和一点对多点的连接。

“蓝牙”的几种典型应用如下：

（1）三合一电话。“蓝牙”技术可以使一部移动电话手机能在多种场合内使用：在办公室里，这部手机是内部电话不计电话费；在家里是无绳电话，计固定电话费；出门在外，是一部移动电话，按移动电话的话费计费。

（2）因特网桥。“蓝牙”技术可以使便携式电脑在任何地方都能通过移动电话手机进入互联网，随时随地到互联网上去“冲浪”。

（3）交互性会议。在会议中“蓝牙”技术可以迅速使自己的信息通过便携式电脑、手机、PDA 等供其他与会者共享。

（4）数码相机中图像的无线传输。“蓝牙”技术将数码相机中的图像发送给其他的数

字相机或者 PC 机、PDA 等。

（5）各种家用设备的遥控和组成家电网络。

3.4.4 超宽频技术（UWB）

超宽频技术（UWB）的发展模式类似 Wi-Fi，有一段很长的时间被归类为军事技术，但如今极有可能扩展至一般消费性产品领域。根据最新的美国联邦通讯委员会（FCC）的定义，超宽频（UWB）系统的中心频率大于 2.5GHz，并具备至少 500MHz 的 -10dB 频宽。频率较低的 UWB 系统必须具备至少 20% 的频宽比（fractional bandwidth）。这些特性让 UWB 明显异于传统的无线电系统，以往的无线电系统的频宽比不会超过 1% 或 20MHz，例如像 2.4GHz 的 IEEE802.11 无线局域网络。

UWB 的历史可回溯至 20 世纪 60 年代，当时发展的主轴为研究微波网络在面对时域脉冲所产生的瞬间行为。在 Harmuth、Ross 以及 Robbins 等研发先锋的努力下，UWB 技术在 20 世纪 70 年代有了重大的发展，其中大部分集中在雷达系统，包括穿地雷达系统。到 20 世纪 80 年代后期，该技术开始被称为无载波或脉冲无线电。美国国防部在 1989 年首次使用超频宽这个名词，在当时 UWB 的理论与技术已经发展将近 30 年之久。自从 1994 年开始，美国大部分的 UWB 研发工作都是在没有分类限制的状况下进行。这种情况大幅加快研发的速度，业界对其商业化发展的兴趣亦大幅提高。

其中有两项发展激发商业界对这项技术的兴趣，包括 UWB 系统可以与其他使用较高频谱密度的通信系统并存，而且不会对其他系统产生干扰；另外 FCC 于 2002 年 2 月 14 日发布的 02-48 号报告与规范，定义各项并存规则，其中包括针对各种类型的 UWB 装置制定电波发射限制。这套法律架构针对各种专利型 UWB 装置立即开拓市场商机，长期而言，市场对标准型产品也有更强烈的兴趣。

由于 UWB 种类众多，因此潜在的用途也相当广泛。其中包括无线局域网络（WLAN）、个人局域网络（PAN）、短距离雷达（例如汽车传感器、防撞系统、智能型高速公路感测系统、液态物体水位侦测系统）、穿地雷达以及应用在医疗监视与运动员训练等领域的人体局域网络。

第一个被排除的主要障碍为美国联邦通信委员会解除 UWB 传输在某些方面的限制。频谱发射上的解禁尤其对高速 PAN 应用的发展特别有利，这类应用涉及影像与多媒体，并已透过 IEEE 工作小组制定的 802.15.3a 规格所标准化。工作小组已在 2002 年 12 月 11 日接获 IEEE 标准委员会的核准，认定新标准符合 5 项审核准则，例如广泛的市场发展潜力、兼容性、明确的定位（代表它涵盖其他标准所没有具备的独特基础）、技术上的可行性以及经济上的可行性。TG3a 计划的时间蓝图已确定，约有 20 家厂商于 2003 年 3 月于达拉斯提出实体层方案。更新版的实体层方案在 2006 年 5 月的 802.15.3a 会议中提出，并将在 2006 年 7 月于旧金山举行的 IEEE 会议中进行决选。如此紧凑的标准化时程反映出下一波支持高速无线功能的数字多媒体消费性装置，的确潜藏着极可观的市场商机。

尽管在无法预测的一段时间内，标准化程序是决定消费者是否会采纳 UWB 技术作为家庭多媒体联机机制的关键因素。但彼此未经协调的 UWB piconet 之间是否能并存运作同样也会产生决定性的影响。面临这种环境加上包括 Philips 在内各大厂商的投入，业界有相当大的动力去找寻一套方法，以能够吸引最终使用者的价位推出标准化的产品。

3.4.5 近距离无线传输（NFC）

NFC（Near Field Communication，近距离无线传输）是由 Philips、NOKIA 和 Sony 主推的一种类似于 RFID（非接触式射频识别）的短距离无线通信技术标准。和 RFID 不同，NFC 采用了双向的识别和连接，在 20cm 距离内工作于 13.56MHz 频率范围。

NFC 最初仅仅是遥控识别和网络技术的合并，但现在已发展成无线连接技术。它能快速自动地建立无线网络，为蜂窝设备、蓝牙设备、Wi-Fi 设备提供一个“虚拟连接”，使电子设备可以在短距离范围进行通信。NFC 的短距离交互大大简化了整个认证识别过程，使电子设备间互相访问更直接、更安全和更清楚，不用再听到各种电子杂音。

NFC 通过在单一设备上组合所有的身份识别应用和服务，帮助解决记忆多个密码的麻烦，同时也保证了数据的安全保护。有了 NFC，多个设备如数码相机、PDA、机顶盒、电脑、手机等之间的无线互连、彼此交换数据或服务都将有可能实现。

此外 NFC 还可以将其他类型无线通信（如 Wi-Fi 和蓝牙）“加速”，实现更快和更远距离的数据传输。每个电子设备都有自己的专用应用菜单，而 NFC 可以创建快速安全的连接，而无需在众多接口的菜单中进行选择。与知名的蓝牙等短距离无线通信标准不同的是，NFC 的作用距离进一步缩短且不像蓝牙那样需要有对应的加密设备。

同样，构建 Wi-Fi 家族无线网络需要多台具有无线网卡的电脑、打印机和其他设备。除此之外，还得有一定技术的专业人员才能胜任这一工作。而 NFC 被置入接入点之后，只要将其中两个靠近就可以实现交流，比配置 Wi-Fi 连接容易得多。

NFC 有如下三种应用类型：

（1）设备连接。除了无线局域网，NFC 也可以简化蓝牙连接。比如，手提电脑用户如果想在机场上网，他只需要走近一个 Wi-Fi 热点即可实现。

（2）实时预定。比如，海报或展览信息背后贴有特定芯片，利用含 NFC 协议的手机或 PDA，便能取得详细信息，或是立即联机使用信用卡进行票券购买。而且，这些芯片无需独立的能源。

（3）移动商务。飞利浦 Mifare 技术支持了世界上几个大型交通系统及在银行业为客户提供 Visa 卡等各种服务。索尼的 FeliCa 非接触智能卡技术产品在中国香港及深圳、新加坡、日本的市场占有率非常高，主要应用在交通及金融机构。

总而言之，这项新技术正在改写无线网络连接的游戏规则，但 NFC 的目标并非是完全取代蓝牙、Wi-Fi 等其他无线技术，而是在不同的场合、不同的领域起到相互补充的作用。所以如今后来居上的 NFC 发展态势相当迅速。

3.5 无线传感网高级关键技术——MAC 协议

图 3-63 所示为符合开放式系统互联模式无线传感网典型协议堆栈 OSI。一般说来，如果参考模型中的各层接口一致定义后，每一层可独立设计。但是为了建立一个可靠并具有严格功耗预算无线自组传感器网络，协议堆栈中的所有层都应满足同样的系统级要求，例如功耗约束、带宽效率、适应性及鲁棒性要求。为使解决方案切实可行，所有层都必须进行设计折中，同时要考虑信道传输能力和设备处理速度等自身的局限性以及 RF 链路质量的变化。

下面对各层协议和平台分别作介绍。

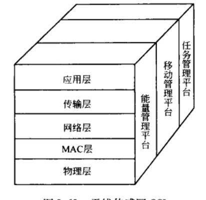


图 3-63 无线传感网 OSI

(1) 物理层（PHY)。它着眼于信号的调制、发送与接收。物理层的主要工作是负责频段的选择、信号的调制以及数据的加密等。对于距离较远的无线通信来说，从实现的复杂性和能量的消耗来考虑，代价都是很高的。

(2) MAC 层。它用于解决信道的多路传输问题。MAC 层的工作集中在数据流的多路技术、数据帧的监测、介质的访问和错误控制，它保证了无线传感网中点到点或一点到多点的可靠连接。

(3) 网络层（NWK)。它关心的是对传输层提供的数据进行路由。大量的传感器节点散布在监测区域中，需要设计 1 套路由协议来供采集数据的传感器节点和基站节点之间的通信使用。

(4) 传输层。它用于维护传感器网络中的数据流，是保证通信服务质量的重要部分。结合无线传感网协议栈图：当传感器网络需要与其他类型的网络连接时，例如基站节点与任务管理节点之间的连接就可以采用传统的 TCP 或者 UDP 协议。但是在传感器网络的内部是不能采用这些传统协议的，这是因为传感器节点的能源和内存资源都非常有限，它需要一套代价较小的协议。

(5) 应用层。根据应用的具体要求的不同，不同的应用程序可以添加到应用层中，它包括一系列基于监测任务的应用软件。

管理平台包括能量管理平台、移动管理平台和任务管理平台。这些管理平台用来监控传感器网络中能量的利用、节点的移动和任务的管理。它们可以帮助传感器节点在较低的能耗的前提下协作完成某些监测的任务。管理平台可以管理一个节点怎样使用它的能量。例如 1 个节点接收到它的一个邻近节点发送过来的消息之后，它就把它的接收器关闭，避免收到重复的数据。同样，一个节点的能量太低时，它会向周围节点发送一条广播消息，以表示自己已经没有足够的能量来帮它们转发数据，这样它就可以不再接收邻居发送过来的需要转发的消息，进而把剩余能量留给自身消息的发送。移动管理平台能够记录节点的移动。任务管理平台用来平衡和规划某个监测区域的感知任务，因为并不是所有节点都要参与到监测活动中，在有些情况下，剩余能量较高的节点要承担多一点的感知任务，这时需要任务管理平台负责分配与协调各个节点的任务量的大小，有了这些管理平台的帮助，节点可以以较低的能耗进行工作，可以利用移动的节点来转发数据，可以在节点之间共享资源。

3.5.1 MAC 协议原理

无线频谱是无线传感网通信介质，是一种无线通信介质，属于稀缺资源。在无线传感网中，可能会有多个节点设备同时接入信道，导致分组之间相互冲突，使接收方无法分辨出接收到的数据，浪费信道资源，吞吐量显著下降。为了解决这些问题，就需要 MAC 层的 MAC 协议。所谓 MAC 协议，就是通过一组规则和过程来更有效、有序和公平地使用共享介质。

在无线传感网中，为了实现多点通信，由MAC（Medium Access Control）介质访问控制层协议决定了局部范围无线信道的使用方式以及多跳自组织无线传感网节点之间的通信资源分配，也就是说必须实现两大基本功能目标：在密集散布的传感器现场能够有助于建立起一个基本网络基础设施所需的数据通信链路；协调共享介质的访问，以便传感器网络节点能够公平有效地分享通信资源。

由于传感器网络独特的资源限制和应用需求，传统的MAC协议不再适合于无线传感网应用范例，如对于一个基于基础设施的蜂窝系统，其MAC协议的设计基本目标是提供高质量的服务质量（QoS）和带宽效率，且主要致力于资源分配策略。而无线传感网没有像基站一样的中央控制机构，况且网络节点的有效节能直接影响无线传感网的使用寿命，因此在设计无线传感网的MAC协议时，有几个方面问题值得重点关注，即能量感知和节省、网络效率（包括公平性、实时性、网络吞吐率和带宽利用率等）、可扩展性。

蓝牙（Bluetooth）及其他自组织网络（MANET）和无线传感网在通信基础设施上有相似的地方，但由于网络寿命的制约，没有哪个现存蓝牙或其他自组织网络MAC协议可以用在无线传感网。

相比之下，除了节能和有效节能外，移动性管理和故障恢复策略也是无线传感网MAC协议首要关注的问题之一。尽管移动蜂窝网络、Ad hoc和蓝牙技术是当前主流的无线网络技术，但它们各自的MAC协议不适合无线传感网。GSM和CDMA中的介质访问控制主要关心如何满足用户的QoS要求和节省带宽资源，能耗是第二位的；Ad hoc网络则考虑如何在节点具有高度移动性的环境中建立彼此间的链接，同时兼顾一定的QoS要求，能耗也不是其首要关心的；而蓝牙采用了主从式的星型拓扑结构，这本身就不适合传感器网络自组织的特点。

目前研究人员针对不同的无线传感网应用，没有采用统一的MAC协议分类方式，但是大体依据标准分为三种，如根据网络拓扑结构方式（分布式和集中式控制）；使用单一或多信道方式；采用固定分配信道还是随机访问信道方式。

将无线传感网MAC协议分为三类，即确定性分配、竞争占用和随机访问。前两者不是传感器网络的理想选择。因为TDMA固定时隙的发送模式功耗过大，为了节省功耗，空闲状态应关闭发射机。竞争占用方案需要实时监测信道状态也不是一种合理的选择。随机介质访问模式比较适合于无线传感网络的节能要求。

根据信道分配使用方式将无线传感网MAC协议分为基于无线信道随机竞争方式和时分复用方式及基于时分和频分复用等其他混合方式三种。

（1）无线信道随机竞争接入方式（CSMA）。节点需要发送数据时采用随机方式使用无线信道，典型的如采用载波监听多路访问（CSMA）的MAC协议，需要注意隐藏终端和暴露终端问题，尽量减少节点间的干扰。

尽管传统的基于CSMA方式的MAC协议也是基于载波监听和退避机制，但它们并不太适合无线传感网，因为它们都基本假设了随机分布的业务，并且趋向于支持独立的点到点的业务流。此外无线传感网MAC协议必须支持可变而且高度相关和可控的周期业务。任意基于CSMA的MAC机制都有两个重要组成部分：监听和退避机制。实际上，无线传感网MAC协议关注的基本问题主要还是能耗管理，而射频通信模块是能耗的最大部件，而MAC协议直接控制射频通信模块，对无线传感网节点节能具有重要的影响。

(2) 无线信道时分复用无竞争接入方式（TDMA）。采用时分复用（TDMA）方式给每个节点分配了一个固定的无线信道使用时段，可以有效避免节点间的干扰。

(3) 无线信道时分/频分/码分等混合复用接入方式（TDMA/FDMA/CDMA）。通过混合采用时分和频分或码分等复用方式，实现节点间的无冲突信道分配策略。

(4) 跳频方式（FHSS）。跳频方式是一种最好的信道分配方式，其实它的原理和 CSMA 的原理近似。但与 CSMA 通信方式比较，跳频通信的灵活性更大，能够更加合理地利用空间资源。在跳频的通信过程中，发送端如果在发送了数据包后，在一定的时间内没有回复，那就说明空气中有相同信道在使用。不会如 CSMA 遇到这样的情况就进入了等待状态，这时跳频就更换频道了，继续尝试有没有回复，如有回复就说明通信成功。这样就可以容易地实现接收和发送端的跳频节奏一致，这样就把通信范围从一个频道扩展到了一个频谱上。

下面介绍几种无线传感网 MAC 协议。

3.5.1.1 S-MAC/DSMAC

W. Ye 等人通过实验证实了无线传感网无效能耗的四大来源：空闲监听，由于节点不知何时邻居节点会向自己发送数据，射频通信模块一直处于接收状态，消耗大量能量；数据冲突，邻居节点同时向同一节点发送多个数据帧，信号相互干扰，接收方无法准确接收，重发数据造成能量浪费；串扰，接收和处理无关的数据；控制开销，控制报文不传送有效数据，消耗节点能量。在 IEEE802.11MAC 协议基础上，W. Ye 等人提出了第一个完全针对无线传感网设计的 MAC 协议 S-MAC（Sensor MAC），具有有效节能、扩展性和冲突避免三大优点。S-MAC 协议对网络做了三大基本假设：拥有很多小的传感器节点；采用 Ad hoc 网络配置；节点致力于协作完成一个或多个共同任务。此外，对于无线传感网应用，S-MAC 协议还假设了网络能够容忍一定的通信延迟；具有较长的空闲周期（直到检测到事件发生为止）；应用关注网络的寿命。针对上面提到的四种能量浪费因素，S-MAC 采用的主要应对机制如下：

(1) 周期监听和睡眠机制。S-MAC 协议将时间分为帧，帧长度由应用程序决定。帧内分监听工作阶段和睡眠阶段。监听/睡眠阶段持续时间根据应用可调，当节点处于睡眠阶段就关掉无线电波以节省能量，但需缓存这期间收到的数据以便工作阶段集中发送并设置一个唤醒定时器。节点还需发送周期同步信息以同步邻居（通过虚拟簇方式），相邻节点也可采用相同的监听/睡眠策略，新节点也可加入进来，节点还需要广播它们各自的监听/睡眠计划，这样使得 S-MAC 具有良好的扩展性。S-MAC 协议采用 RTS/CTS/DATA/ACK 机制发送数据，发送数据期间不会进入睡眠阶段。该机制存在不足的是由于采用周期睡眠会带来一定的通信延迟，此外会占用大量存储空间缓存数据，这在资源受限的无线传感网显得尤为突出，图 3-64 所示给出了 S-MAC 协议周期性监听和睡眠。

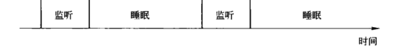


图 3-64 S-MAC

（2）冲突和串音避免机制。为了减少冲突和避免串音，S-MAC 采用了物理和虚拟载波（使用网络分配矢量 NAV）监听机制和 RTS/CTS 握手交互机制。与 IEEE802.11MAC 协议不同的是当邻居节点正在通信时，S-MAC 协议节点直接进入睡眠阶段；当接收方节点处于空闲并正在监听周期时，就会被唤醒。串音分组通常是不需要的分组，它随着节点密度和业务负载增加而变得更加严重，因而造成能量浪费。串音可以通过更新基于 RTS/CTS 的 NAV 来避免，当 NAV 不为零就进入睡眠阶段，从而避免串音现象发生。一个可以遵循的原则就是当发送方和接收方的所有邻居在节点发送数据期间监听到 RTS/CTS 后就应当进入睡眠阶段。

（3）消息传递机制。S-MAC 协议采用了消息传递机制以很好地支持长消息的发送。对于无线信道，传输差错和消息长度成正比，短消息传输成功的概率要大于长消息。消息传递技术根据这一原理，将长消息分为若干个短消息，采用一次 RTS/CTS 交互的握手机制预约这个长消息发送的时间，集中连续发送全部短消息，既可以减少控制报文开销，又可以提高消息成功发送率。IEEE802.11MAC 与 S-MAC 协议不同的是考虑了网络的公平性，RTS/CTS 只预约下一个短消息发送的时间，其他节点在每个短消息发送完成后都不需醒来进入监听工作阶段，只要发送方没有收到某个短消息的应答，连接就会断开，其他节点便可以开始竞争信道。

（4）流量自适应监听机制。在多跳无线传感网中，节点周期性睡眠会导致通信延迟的累加。S-MAC 协议采用了流量自适应监听机制，减小了通信延迟的累加效应。主要思想就是在一次通信过程中，通信节点的邻居节点在通信结束后不立即进入睡眠阶段，而是保持监听一段时间。如果节点在该时间段内收到 RTS 分组，则可立即接收数据，无需进入下一次监听工作周期，从而减少了数据分组的传输延迟。如果这段时间没有收到 RTS 分组，则转入睡眠阶段直到下一次监听工作周期。

DSMAC 协议是在 S-MAC 协议基础上引入了动态工作周期特征，旨在减少延迟敏感应用的传输延迟。在 SYNC 同步期间，所有节点共享一跳的延迟值（指当接收到进入队列的一个分组与其传输之间的时间间隔），且开始都是相同的工作周期。当一个接收节点发现平均一跳延迟值较高时，就决定缩短其睡眠时间并在 SYNC 期间广播该消息。对应地，当发送节点收到睡眠时间缩短信号，则检查其队列的发往接收方的分组。如果存在一个分组且电池高于规定的阈值时，就决定将其工作周期加倍。

DSMAC 协议工作周期加倍后使得邻居的调度将不受影响。这样其传输延迟要优于 S-MAC协议的延迟。此外，对于每个分组而言，DSMAC 协议拥有更低的平均功耗。

3.5.1.2 T-MAC

T-MAC（Timeout-MAC）协议是在 S-MAC 协议基础上改进的，也将时间分为帧，帧长度固定，监听工作长度可变。作者认为空闲监听的能耗占前面提到的四种无效能耗中绝对大的比例，特别是在消息传输频率较低的情况下。

T-MAC 协议规定了五种事件和一个计时器 TA，根据 TA 确定监听工作阶段的结束时间。五种事件分别是：帧长度超时，即周期时间定时器溢出；节点在无线信道收到数据；通过接收信号强度指示 RSSI 感知数据传输冲突；节点的数据或确认发送完成；通过监听 RTS/CTS 确认邻居节点完成数据交换。如果在 TA 内，通信模块没有监听到这五种事件中

的任何一种，就认为信道进入空闲状态。节点就关闭无线电波通信模块，进入睡眠阶段。为了减少空闲监听能耗，可以采用低能耗监听技术。

T-MAC 协议节点周期性地短时间监听信道，以确定信道空闲状态。如果无线信道空闲，节点再次进入睡眠阶段。如果信道忙，节点继续监听信道，直到数据接收完毕或信道再次空闲。节点在发送数据时，帧前加入唤醒前导，使得接收节点在帧的数据部分发送前进入工作状态，以接收数据。加入唤醒前导，增加了发送和接收数据的控制开销，但减少了空闲监听的能耗。S-MAC 协议的周期长度受限于应用延迟要求和节点缓存大小，活动时间主要依赖于消息速率。这样就存在一个问题：延迟要求和缓存大小通常都是固定的，而消息速率是变化的。如果要保证及时可靠的消息传输，节点活动时间必须适应最高通信负载。当负载较小时，节点处于空闲监听时间相对增加。

针对此问题，T-MAC 协议在保持周期长度不变的基础上，根据通信流量动态调节活动时间，用突发方式发送消息，从而减少空闲监听时间。相对于 S-MAC，T-MAC 协议减少了处于活动阶段的时间。在每个活动阶段的开始，T-MAC 按照突发方式发送所有数据，其中 TA 决定每个周期最小的空闲监听时间，它的取值对于整个协议性能至关重要。

由于无线传感网存在业务汇聚的数据单向通信情况，T-MAC 协议存在一种特殊的通信延迟，即早睡（Early-sleep Problem）问题。假设节点 A 沿路线 $A \to B \to C \to D$ 传输数据到节点 D。如节点 A 首先获得竞争优先权发送数据 RTS 消息给节点到 B，B 收到 RTS 后应答 CTS 消息。节点 C 收到 B 发出的 CTS 消息立即转入睡眠阶段，等节点 B 接收完数据才醒来，以便接收节点 B 发给它的数据。D 由于不知道节点 A 和 B 之间的通信存在，故节点 $A \to B$ 的通信结束后就处于睡眠阶段，节点 C 只有等到下一个工作周期才能传数据给节点 D，这样就存在一个通信延迟，即早睡现象。

为克服上面的目的节点早睡问题，T-MAC 协议又提出了两种解决方案：第一种方法是在节点 C 和 A 分别引入 FRTS（Future Request-To-Send）和 DS（Data-Send）分组。节点 C 收到 B 发给 A 的 CTS 分组后立即向下一跳节点 D 发出 FRTS，其中包含 D 接收数据前需等待的时间，节点 D 必须睡眠该等待时间后才能唤醒接收数据。节点 A 收到 CTS 分组后需发送一个与 FRTS 等长度的分组 DS 才能实现对无线信道的占用，节点 A 在 DS 分组之后就可发送数据消息了。尽管 FRTS 方法提高了数据吞吐率，但带来了额外的分组 FRTS 和 DS 通信开销。第二种方法就是满缓冲区优先策略（Full Buffer Priority）。当节点缓冲区快要满时，对收到的 RTS 不予应答，而立即向目标接收者发送 RTS 消息，并传输数据给目标节点。该方法优点是减小早睡问题发生的可能性，起到一定网络流量控制作用，然而增加了网络冲突的可能性。

3.5.1.3　Sift

Sift 协议是 K. Jamieson 等提出的基于事件驱动的无线传感网 MAC 协议，不同于上面 IEEE802.11 和其他基于竞争的 MAC 协议，它充分考虑了无线传感网的三个特点：大多数传感器网络是事件驱动的网络，因而存在事件检测的空间相关性和事件传递的时间相关性；由于汇聚节点的存在，不是所有节点都需要报告事件；感知事件的节点密度随时间动态变化。

Sift 协议设计的目的是当共享信道的 N 个传感器节点同时监测到同一事件时，希望 R

个节点（$R \leqslant N$）能够在最小时间内无冲突地成功地发送事件检测消息，抑制剩余 $N\text{-}R$ 个节点的消息发送。Sift 协议不但保留了 S-MAC 和 T-MAC 协议都具有的尽可能让节点处于睡眠阶段以节省能量的功能。而且，由于无线传感网的流量具有突发性和局部相关性，Sift 协议很好地利用了这些特点，通过在不同时隙采用不同的发送概率，使得在短时间内部分节点能够无冲突地广播事件，从而在节省能量的同时也减少了消息传输的延迟，这是和以往的 MAC 协议最大不同之处。

通常一般的基于窗口的竞争性 MAC 协议中，当有数据需要发送时，节点首先在发送窗口$[1, CW]$内的概率随机选择一个发送时隙；然后节点监听直到选择的发送时隙到来。如监听期间没有其他节点使用信道，则节点立即发送数据，否则需在信道空闲时重新选择发送时隙。当多个节点选择相同一个时隙时就会发生冲突。多数协议都是规定冲突节点倍增 CW 值，并在新窗口内重新选择发送时隙，以增大无冲突发送的概率。

但是这种方法使无线传感网存在新的问题：当多个节点同时监测到同一事件，并同时发送数据时，导致事件区域内节点同时闲忙，忙时竞争加剧，需要经过很长时间来调整 CW 值，以适应发送节点的数目；如果 CW 值很大，而同时监测同一事件的节点数目很少时，就会造成报告事件的延迟较大。此外 CW 取值是为了保证所有活动节点都有机会发送数据，而无线传感网只需 N 个活动节点中有 R 个节点能够无冲突地报告事件。Sift 协议采用的是 CW 值固定的窗口，节点不是从发送窗口选择发送时隙，而是在不同时隙中选择不同发送数据的概率。因此，关键在于如何在不同时隙为节点选择合适的发送概率分布，使得监测到同一事件的多个节点能够在竞争窗口前面各个时隙内无冲突地发送数据消息。

Sift 协议工作过程如下：当节点有消息发送时，首先假定当前有 N 个节点与其竞争发送。如果在第一个时隙内节点不发送消息，也无其他节点发送消息，则节点就减少假想的竞争发送节点的数目，并相应地增加选择在第二个时隙发送数据的概率；如果节点没有选择第二个时隙，且无其他节点在该时隙发送消息，则节点继续减少假想的竞争发送节点数目，并进一步增加选择第三个时隙发送数据的概率。依次类推，节点在选择第 r 个时隙发送数据的概率 P_r 为：

$$P_r = \frac{(1-\alpha)\alpha^{CW}}{1-\alpha^{CW}}\alpha^{-r}, r = 1, \cdots, CW \tag{3-1}$$

式中，α 为分布参数（$0<\alpha<1$）。如果选择时隙过程中有其他节点发送消息，节点就进入重新开始竞争过程。Sift 协议就是通过非均匀概率分布将优胜节点从整个竞争节点中筛选（Sift）出来的。式（3-1）中参数 α 选择与 N 和 CW 值相关。

Sift 协议和 S-MAC 以及 T-MAC 协议一样只是从发送数据的节点考虑问题，对接收节点的空闲状态考虑较少，需要节点间保持时钟同步，特别适合于传感器网络内局部区域使用，如分簇结构网络。簇头可以一直处于监听状态，这样节点发送消息给一直处于活动状态的簇头节点，通过簇头节点的能量消耗换来消息传输延迟的缩短。

3.5.1.4 WiseMAC

由于 T-MAC 协议在帧前加入了唤醒前导，这样就引入了控制开销。为了将控制开销压缩到最小，WiseMAC 协议在数据确认分组中携带了下一次信道监听时间，节点获得所有邻居节点的信道监听时间。在发送数据时可以将唤醒前导压缩到最短。

考虑节点时钟的漂移，唤醒前导长度 $TP = \min(4\theta L, TW)$。其中，θ 是节点的时钟漂移速度；L 是从上次确认分组到现在的时间；TW 是所有节点监听信道的时间间隔。尽管 WiseMAC 协议能够很好地适应网络流量的变化，但是节点需要存储邻居节点的信道监听时间，会占用大量存储空间，并增加协议实现的复杂度，对于高密度的无线传感网，该问题较为突出。

3.5.1.5 B-MAC

B-MAC（Berkeley-MAC）协议采用信道估计和退避算法分配信道，通过链路层保证传输可靠性，利用低功耗技术减少空闲监听，实现低功耗通信。

信道估计凭借对接收信号强度指示 RSSI，采用指数加权移动平均算法计算出信道的平均噪声，再将一小段时间内的最小 RSSI 值与平均噪声相比较，从而确定信道的冲突状态。退避算法根据应用需求可以选择初始退避和拥塞退避两种方式。

3.5.1.6 IEEE802.15.4MAC 协议

IEEE802.15.4 为无线传感网的应用提供了一种低成本、低功耗和低速率的无线联网的标准。该标准不但定义了物理层，即可以有三种频率选择（2.4GHz、915MHz 和 868MHz），而且也规定了 MAC 层协议采用 CSMA/CA 的竞争性接入方式。

为降低功耗，采用了缓存节能机制，节点周期监听信道，接收信标（Beacon）帧，当没有数据接收和发送时就进入睡眠阶段。网络协调者暂时缓存发往睡眠节点的数据，并定期发送信标帧，信标帧携带了这些缓存数据的目的节点的地址。当节点发现网络协调者缓存了发往自己的数据之后，向其发送轮询帧（Poll），表明自己可接收数据了。当网络协调者收到轮询帧后，首先向节点发送确认帧（ACK），然后发送缓存的数据。收到数据后，节点再向网络协调者发送确认帧。

3.5.1.7 BMA 协议

BMA 协议适合于分簇的无线传感网，分为簇建立和稳定两个阶段。在簇建立期间，节点是根据剩余能量多少来选择簇头节点的。所有当选簇头通过非持续的 CSMA 方式向其他节点广播当选通告。其他节点收到通告后根据接收信号强度决定加入哪一个簇。经过一段时间系统进入稳定工作阶段。该阶段由若干定长的会话组成，每个会话包括竞争阶段、数据传输阶段和空闲阶段。竞争阶段所有节点都打开通信模块，竞争数据传输阶段。

竞争阶段之后，簇头建立数据发送调度策略并向簇内节点广播数据发送调度策略，这样每个需要发送数据的节点获得了一个确定的发送时间。各个节点只有在自己的发送时间内打开通信模块，向簇头发送数据，其余时间都转入睡眠阶段。如果一个长会话内没有节点发送数据，那么数据传输阶段长度为 0。簇头收到簇内节点数据后，需要进行数据融合，并向汇聚节点发送。相比于传统的 TDMA 和有效节能的 TDMA 协议（节点在分配给它的时隙里没有数据发送就将无线电通信模块关掉），BMA 协议最大的贡献就是使得平均分组延迟大大减小。

此外，除了上面主要关注节能和延迟的 MAC 协议外，Woo 和 Culler 提出了一个新的基于 CSMA 的无线传感网的 MAC 竞争协议，考虑了有效节能和公平性问题，没有引入额

外的控制分组开销，并从仿真实验证实了采用固定的监听周期策略且在退避期间关掉无线电波方式较为节能，而且引入随机延迟使得无线传感网对于避免数据的反复冲突提供了鲁棒性。他们还提出了一种自适应传输速率控制机制，实现了公平性和较好的吞吐性能。

3.5.2 MAC 硬件支持和物理（PHY）层

无线传感网不同层通过服务接入点进行通信，大多数层有两个接口：数据实体接口和管理实体接口。数据实体接口的目标是向上层提供所需的常规数据服务；管理实体接口的目标是向上层提供访问内部层参数、配置和管理数据的机制。

PHY 层由射频收发器以及底层的控制模块组成，定义了物理无线信道和 MAC 层之间的接口，主要功能是启动和关闭无线收发器、能量监测、链路质量监测、信道选择、清除信道评估以及通过物理介质对数据包进行发送和接收。

MAC 层为高层访问物理信道提供了点到点通信的服务接口，具体功能是信标管理、信道接入、时隙管理、发送确认帧、发送连接及断开连接请求，此外，MAC 层还为应用合适的安全机制提供了一些方法。

网络层主要用于建立和维护网络连接它独立处理传入数据的请求，关联、解除关联和孤立通知请求。应用层主要为无线传感网技术的实际应用提供一些应用框架模型等，以便对无线传感网技术进行开发应用。

能耗和成本是无线传感网最主要的两个性能指标，也是指导 WSN 物理层协议设计的关键因素。

WSN 低能耗的要求同时也带来了能源选择问题。目前，WSN 的主要能源仍然是传统的电池。但是如何根据 WSN 的工作特点选择适合的电池也是一个研究重点。脉冲放电电池适合低负载周期 WSN，并可采用充电恢复效应来延长该电池的寿命。同时，由于 WSN 无人值守的特点，一些可靠地从周围环境取得能量并将其转换成微瓦电能的方法受到了广泛的关注。其中，振动和应变形式的光能、热能和机械能是最有可能的能量来源。然而，这些能源都有各自的局限性，例如太阳能设备需要光，机械能则需要动力。因此 WSN 非传统能源的研究也是值得关注的问题。

成本是 WSN 广泛应用的前提，而包含硬件的物理层成本决定网络的成本。为了降低成本，物理层的设计应该遵循以下原则：

（1）集成。集成化的产品无需考虑其他外置部件，无疑可以降低成本。对于 WSN 节点，天线和电源是最难集成的元件，目前还未实现。其次是石英水晶基频，在对基频的稳定性要求不高的情况下，可以考虑采用微机电系统（MEMS）共鸣器替代离散石英水晶基率。

（2）选择数字元件。为了实现低成本集成，需要考虑如何选择模拟和数字电路。众所周知，与模拟电路相比，数字电路的集成使用印刷电路板，体积较小，成本较低，因此尽可能采用数字电路是理想的方案。在所有元件中，最难选择电路类型的是接收器信道滤波器，若采用模拟电路，则体积较大，而若采用数字电路，则需要增加一假频滤波器和一数模转换器。由于模拟信道滤波器的大小与滤波器的转角频率成反比，因此设计中应该考虑如何在信道滤波器的转角频率和 IC 成本之间取得折中。

（3）协议简单化。实现低成本要求尽量降低所设计的协议、算法的复杂度，从而降低

对硬件的要求。

物理层协议涉及 WSN 采用的传输媒体、选择的频段以及调制方式。目前，WSN 采用的传输媒体主要包括无线电、红外线和光波等。

无线电波易于产生，传播距离较远，容易穿透建筑物，在通信方面没有特殊的限制，比较适合 WSN 在未知环境中的自主通信需求，是目前 WSN 的主流传输方式。

在频率选择方面，一般选用工业、科学和医疗（ISM）频段。选用 ISM 频段的主要优点是 ISM 频段是无需注册的公用频段，具有大范围的可选频段，没有特定的标准，可以灵活使用，面对传感器节点小型化、低成本、低功耗的特点。在美国可用的免许可证的频带包括：27MHz、260 ~ 470MHz、902 ~ 928MHz 和最常用的 2.4GHz 频带。其中 260 ~ 470MHz 频带对数据传送的类型有所限制，而其他频带则没有这样的限制。ISM 频道在欧洲所分配到的频率为 433MHz、868MHz 和 2.4GHz。中国目前可以使用的 ISM 频率是：433MHz 和 2.4GHz。国际通用的频段为 2.4GHz。

在调制机制选择方面，传统的无线通信系统需要考虑的重要指标包括频谱效率、误码率、环境适应性以及实现的难度和成本。在 WSN 中，由于传感器节点能量受限，需要设计以节能和成本为主要指标的调制机制。为了同时满足 WSN 最小化符号率和最大化数据传输率的指标，M-ary 调制机制被应用于 WSN。

然而简单的多相位 M-ary 信号将降低检测的敏感度，为了恢复连接，则需要增加发射功率，因此导致额外的能量浪费。为了避免该问题，准正交的差分编码位置调制方案，采用四位二进制符号，每个符号被扩展为 32 位伪噪声 CHIP，采用半正弦脉冲波形的偏移四相移键控（OQPSK）调制机制，仿真实验表明该方案的节能性较好。M-ary 调制机制通过单个符号发送多位数据的方法减少了发射的时间，降低了发射功耗，但是所采用的电路很复杂，无线收发器的功耗比较大。如果以无线收发器的启动时间为主要条件，则 Binary 调制机制在启动时间较长的系统中更加节能、有效，而 M-ary 调制机制适用于启动时间较短的系统。一种基于直序扩频—码分多路访问（DS-CDMA）的数据编码与调制方法，该方法通过使用最小能量编码算法来降低多路访问冲突，减少能量消耗。

另外，UC Berkeley 研发的 PicoRadio 项目采用无线电唤醒装置，该装置支持睡眠模式，由包含目的节点 ID 的唤醒信标唤醒目的节点并通知其切换到相应的信道，从而实现在全负载周期运行时的能耗小于 100pW，DARPA 资助的 WINS 项目研究如何采用 CMOS 电路技术实现硬件的低成本制作。AIT 研发的 μAMPS 项目在物理层设计时考虑了收发机在从睡眠模式到工作模式的转换能量大于工作时消耗的能量。

WSN 物理层协议的实现可以基于 IEEE 的标准——IEEE802.15.4。

IEEE 于 2002 年开始研究制订低速无线个人局域网（WPAN）标准——IEEE802.15.4，IEEE802.15.4 主要是物理层和 MAC 层标准，IEEE1451 工作组正在考虑以此为基础实现传感器网络（Sensor Network），IEEE802.15.4 标准主要有如下特性：

（1）工作于 2.4GHz ISM 频段的 16 个信道，915MHz 频段的 10 个信道以及 868MHz 频段的 1 个信道。

（2）2.4GHz 频段提供的数据传输率为 250kb/s，适用于较高的数据吞吐量、低延时或低作业周期的场合。868/915MHz 频段提供的数据传输率为 20kb/s、40kb/s，用较低的速率换取较高的灵敏度和较大的覆盖面积。

（3）2.4GHz 物理层采用如前所述的基于 DSSS 方法的准正交调制技术，868/915MHz 物理层使用简单 DSSS 方法，每个数据位被扩展为长度为 15 的 CHIP 序列，然后使用二进制相移键控调制技术。

（4）采用 CSMA-CA 信道接入技术，以及两种寻址方式——短 16 位比特和 64 位比特寻址。

（5）保证低功耗的电源管理。

WSN 无人值守、能量受限等特点给其物理层的实现带来了很多的困难。

目前的 WSN 节点在体积、成本和功耗上与其广泛应用的标准还存在一定的差距，小型化、低成本、低功耗的片上系统（SOC）正在逐步进入市场，如 TI 公司的 CC2430、CC2431、CC2530 及 Freescale 公司的 MC13224 等。

细胞计算是实现纳米级组装的新技术，也为 WSN 的研究提供了新的思路。

WSN 物理层迫切需要符合其特点和要求的简单的协议、算法设计，特别是调制机制。

3.5.3 典型 MAC 和网络层接口

网络层的主要功能就是提供一些必要的函数，确保 MAC 层正常工作，并且为应用层提供合适的服务接口，如图 3-65 所示。为了向应用层提供其接口，网络层提供了两个必需的功能服务实体，它们分别是数据服务实体和管理服务实体，如图 3-65 所示。网络层数据实体通过网络层数据实体服务接入点（NLDE-SAP）提供数据传输服务，网络管理层实体通过网络层管理实体服务接入点（NLME-SAP）提供网络管理服务。网络层管理实体利用网络层数据实体完成一些网络的管理工作，并且网络层管理实体完成对网络信息库（NIB）的维护和管理。

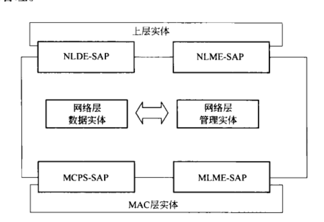


图 3-65 网络层参考模型

网络层通过 MCPS-SAP 和 MLME-SAP 接口为 MAC 层提供接口。通过 NLDE-SAP 与 NLME-SAP 接口为应用层提供接口服务。

网络层负责路由查找和数据包传送。自组传感器网络中大量节点是随机部署的，因此在网状网中查找多跳路由十分困难，当节点出现故障或重新部署后进行路由维护和修复（自愈）将同样困难。大量可支持自组多跳网络的分布式路由算法可分为两类，即主动式

(proactive) 和被动式 (reactive)。在主动式路由协议中，网络中的所有节点都常常保持着源地址与目的地址之间的路由列表，而不管是否需要这些路由。

由于无须花时间查找路由，主动式路由能比被动式路由更快地传输数据包。不过，随着网络规模增加，这些路由列表也呈指数级增加，因此对于包含大量节点的典型传感器网络来说，要继续保持这些列表十分困难。而在被动式路由协议中，源节点只有在需要向某个目的节点传输数据时才开始查找路由。找到路由后该节点会将路由信息保持一定时间。路由列表规模相对较小，与网络规模大致相同。不过查找路由通常会有较长的延时，在要求实时性的应用中不可采用。

多数自组移动网采用的分布式路由算法都是基于网状网等平面网络结构而开发的，而无论是主动式路由还是被动式路由，由于自组网不分层，每个节点都充当其他节点的中继，其承担的责任相同。在这种采用全分布式路由算法的平面网络中，不进行传输的所有节点都必须主动监听信道，以实现中继。因此网状网中的分布式路由算法产生较高的功耗。使用星型—网状混合结构可开发一种智能路由，实现高功效、降低延时并增强连接性。由于每个传感器的路由列表存储空间有限，被动式路由可为传感器网络应用提供更紧凑的解决方案。通过将信息传输到充当数据集中站的少量节点上，可有效解决被动式路由的延时问题。每个集中站负责收集邻近区域的通信信息。

将通信保持在局部邻近范围内十分重要，它可保证自组网的可伸缩性。据观察，每个节点的传输能力随着自组网规模增加而下降，这是因为网络规模增大后，源节点与目的节点间的平均路径长度也成比例增加。为了避免大型网络中节点的传输能力逐渐降低，网络中所有通信都应当保持在局部区域内，即数据包的平均跳跃次数应该比网络的总中继数少。

3.5.4 IEEE802.15.4 规范 MAC 标准

IEEE802 系列标准把数据链路层分成逻辑链路控制 (Logical Link Control, LLC) 和 MAC 两个子层。LLC 子层在 IEEE802.6 标准中定义，为 802 标准系列所共用；而 MAC 子层协议则依赖于各自的物理层。IEEE802.15.4 的 MAC 子层能支持多种 LLC 标准，通过业务相关汇聚子层 (Service-Specific Convergence Sub layer, SSCS) 协议承载 IEEE802.2 协议中第一种类型的 LLC 标准，同时也允许其他 LLC 标准直接使用 IEEE802.15.4MAC 子层的服务。

LLC 子层的主要功能是进行数据包的分段与重组以及确保数据包按顺序传输。

IEEE802.15.4MAC 子层实现包括设备间无线链路的建立、维护和断开，确认模式的帧传送与接收，信道接入与控制，帧校验与快速自动请求重发 (ARQ)，预留时隙管理以及广播信息管理等。MAC 子层处理所有物理层无线信道的接入，主要功能有：(1) 网络协调器产生网络信标；(2) 与信标同步；(3) 支持个域网 (PAN) 链路的建立和断开；(4) 为设备的安全提供支持；(5) 信道接入方式采用免冲突载波检测多址接入 (CSMA-CA) 机制；(6) 处理和维护保护时隙 (GTS) 机制；(7) 在两个对等的 MAC 实体之间提供一个可靠的通信链路。

MAC 子层与 LLC 子层的接口中用于管理目的的原语仅有 26 条，相对于蓝牙技术 131 条原语和 32 个事件而言，IEEE802.15.4MAC 子层的复杂度很低，不需要高速处理器，因

此降低了功耗和成本。

MAC 层在服务协议汇聚层（SSCS）和物理层之间提供了一个接口。MAC 层包括一个管理实体，该实体通过一个服务接口可调用 MAC 层管理功能，该实体还负责维护 MAC 层固有的管理对象的数据库。从图 3-66 可以看到在 MAC 层两个不同服务的接入点提供两不同 MAC 层服务。MAC 层通过它的公共部分子层服务接入点为它提供数据服务；MAC 层通过它的管理实体服务接入点为它提供管理服务。

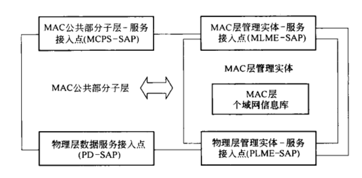


图 3-66 MAC 层参考模型

图 3-67 给出了 MAC 子层数据包格式。MAC 子层数据包由 MAC 子层帧头（MAC Header，MHR）、MAC 子层载荷和 MAC 子层帧尾（MAC Footer，MFR）组成。MAC 子层帧头由 2 字节的帧控制域、1 字节的帧序号域和最多 20 字节的地址域组成。帧控制域指明了 MAC 帧的类型、地址域的格式以及是否需要接收方确认等控制信息；帧序号域包含了发送方对帧的顺序编号，用于匹配确认帧，实现 MAC 子层的可靠传输；地址域采用的寻址方式可以是 64b 的 IEEE MAC 地址或者 8b 的 ZigBee 网络地址。

2 字节	1 字节	0/2 字节	0/2/8 字节	0/2 字节	0/2/8 字节	可变	2 字节
帧控制	序列号	目的 PAN 标识符	目的地址	源 PAN 标识符	源地址	帧载荷	FCS
MHR（MAC 层帧头）						MAC 载荷	MFR

图 3-67 MAC 层数据包格式

MAC 子层载荷，其长度可变，不同的帧类型帧包含有不同的信息（如 MAC 子层业务数据单元（MAC Service Data Unit，MSDU），但整个 MAC 帧的长度应该小于 127 字节，其内容取决于帧类型。IEEE802. 15. 4 的 MAC 子层定义了四种帧类型，即广播（信标）帧、数据帧、确认帧和 MAC 命令帧。只有广播帧和数据帧包含了高层控制命令或者数据，确认帧和 MAC 命令帧则用于 ZigBee 设备间 MAC 子层功能实体间控制信息的收发。

MAC 子层帧尾含有采用 16b CRC 算法计算出来的帧校验序列（Frame Check Sequence，FCS），用于接收方判断该数据包是否正确，从而决定是否采用 ARQ 进行差错恢复。广播帧和确认帧不需要接收方的确认，数据帧和 MAC 命令帧的帧头包含帧控制域，指示收到

的帧是否需要确认，如果需要确认，并且已经通过了 CRC 校验，接收方将立即发送确认帧。若发送方在一定时间内收不到确认帧，将自动重传该帧，这就是 MAC 子层可靠传输的基本过程。

IEEE802.15.4MAC 子层定义了两种基本的信道接入方法，分别用于两种 ZigBee 网络拓扑结构中。这两种网络结构分别是基于中心控制的星型网络和基于对等操作的网状网络。在星型网络中，中心设备承担网络的形成和维护、时隙的划分、信道接入控制和专用带宽分配等功能，其余设备根据中心设备的广播信息来决定如何接入和使用无线信道，这是一种时隙化的载波侦听和冲突避免（Carrier Sense Multiple Access with Collision Avoidance，CSMA/CA）信道接入算法。在对等网状方式的网络中，没有中心设备的控制，也没有广播信道和广播信息，而是使用标准的 CSMA/CA 信道接入算法接入网络。

3.5.5 采用 MAC 建立星状自组织无线传感网

IEEE802.15.4 标准适用于低速率、低功耗、低复杂度和短距离数据传输的无线个域网（WPAN）。在网络内的无线传输过程中，采用带冲突避免的载波侦听多路访问机制（CSMA/CA），支持超帧结构和时槽保障机制（GTS）。网络拓扑结构可以是星型网或点对点的对等网。该标准定义了 3 种数据传输频率，分别为 868MHz、915MHz、2.4GHz。前两种传输频率采取 BPSK 调制方式，后一种采取 0-OPSK 的调制方式。各种频率分别支持 20kb/s，40kb/s 和 250kb/s 的无线数据传输速率，传输距离在 0 ~ 70m 之间。本节中采用的是频率为 2.4GHz 的无线收发模块。

无线传感网平台由光强传感器模块、微处理器模块、无线发射模块三个部分组成，如图 3-68 所示。微处理器模块和无线发射模块集成在一块板子上，而光强传感器模块通过接口与微处理器相连，这样可以通过更换不同的传感器模块来应用于各种场合。

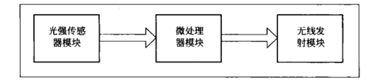


图 3-68 平台

由于各种不同的应用场合中需要采集的模拟量千变万化，网络平台中传感器模块采用了拥有 20 针插针的通用接口。这样可以通过更换不同的传感器模块子板来应用于各种场合。传感器电路部分设计采用技术在无数据采集任务时降低功耗。

微处理器及无线发射模块采用的是飞思卡尔（Freescale）公司 MC13224，是第三代 ZigBee 解决方案，集成了完整低功耗 2.4GHz 无线电收发器，基于 32 位 ARM7 核的 MCU，用于 IEEE802.15.4、MAC 和 AES 安全加密的硬件加速器以及 MCU 成套外设，是高密度低元件数 IEEE802.15.4 综合解决方案，能实现点对点连接和完整的 ZigBee 网状网络，因此可广泛应用在住宅区和商业自动化、工业控制、HVAC、卫生保健和消费类电子等产品。

MC13224 支持国际 802.15.4 标准以及 ZigBee、ZigBee PRO 和 ZigBee RF4CE 标准。提供了 104dB 的链路质量，优秀的接收器灵敏度和健壮的抗干扰性，多种供电模式，以及一

套广泛的外设集——包括 2 个高速 UART、12 位 ADC 和 64 个通用 GPIO，4 个定时器，I2C 等。除了更强 MCU，改进了 RF 输出功率、灵敏度、选择性，且一般会提供一个超越上一代 CC2430 的重要性能改进。除了通过优秀的 RF 性能、选择性和业界标准 ARM7TDMI-S 内核，支持一般低功耗无线通信，还可以配备一个标准网络协议栈（ZigBee RF4CE，ZigBee）来简化开发，使你更快地获得市场。

该芯片只需极少外部元器件，性能稳定且功耗极低。MC13224 选择性和敏感性指数超过了 IEEE802. 15. 4 标准的要求，可确保短距离通信的有效性和可靠性。

在本节中无线传感网采取星型拓扑结构，由一个网络协调器作为中心节点，可以跟任何一个普通节点通信。普通节点上含有光强传感器对周围环境中的光信号强度参数进行测量、采样，将采集到的数据发往中心节点，并且可以对中心节点发来的数据、命令进行分析处理，完成相应的操作。若两个普通节点之间要传送数据则必须经过中心节点，由中心节点把数据传送到相应的节点上。

无线传感网是一个自组织的网络，如果一个全功能节点被激活，它就可能建立一个网络并把自己设为网络协调器，其他的普通节点可以申请加入该网络。这样就可以建成一个具有星型拓扑结构的无线传感网。本节中的无线传感网支持超帧结构，网络协调器经过能量扫描、主动信道扫描后，按照设定的参数周期性地发送信标帧。普通节点首先经过能量扫描和被动信道扫描后，获取信标帧中包含网络特征的参数，如信标序号（beaconorder）、超帧序号（superFrameorder）和网络标号等。通过 mlmeSyncRequest（）函数（根据 MLME-SYNC. request 原语编写）请求与网络协调器同步，再通过 mlmeAssociateRequest（）函数（根据 MLME-ASSOCIATE. request 原语编写）请求与网络协调器关联。在与网络协调器关联的过程中，网络协调器为每个请求关联的普通节点分配 16 位的短地址。这样在以后的数据传送中就可以用短地址进行通信，提高通信效率、降低发射中的能量消耗，从而延长网络的使用寿命。

在 IEEE802. 15. 4 标准中定义了四种帧，分别是信标帧、数据帧、命令帧、确认帧。纯灯光控制的无线传感网中，这四种帧都得到了应用。

（1）信标帧：用以网络协调器在支持超帧结构的第一个时槽向其邻近节点广播信标，当附近的节点接受到信标帧后就可以申请加入该网络。信标帧的结构如图 3-69 所示，在帧控制域中定义了帧的类型为信标帧。

字节：2	1	4	2	可 变	可 变	2
帧控制域	序列号域	地址域	超帧描述字段	转发数据地址	信标负载	FCS

图 3-69 信标帧

由于本节中的无线传感网系统采用相对简单的星型拓扑结构，在信标帧的结构上与 IEEE802. 15. 4 标准有所不同：在信标帧的地址域中已包含源节点的网络标号和短地址，不包含目的节点信息（因为采用广播方式发送）。在信标帧中没有 GTS 域，不支持时槽保障机制。

（2）数据帧：用来传送含有光强度信息的数据。数据帧的结构如图 3-70 所示，在帧控制域中定义了帧的类型为数据帧。

字节：2	1	8	1	1/20	2
帧控制域	序列号域	地址域	负载长度域	数据帧负载	FCS

图 3-70 数据帧

在地址域中包含源节点和目的节点的网络标号和短地址。由于数据帧的传送方向有两种，即从普通节点传向中心节点和从中心节点发送给普通节点。它们的数据负载域的长度不同，分别为 20 字节和 1 字节。

（3）命令帧：用于组建无线传感网、传输同步数据等。命令帧在格式上和其他类型的帧没有太多的区别，其结构如图 3-71 所示。

字节：2	1	8/14	1	可 变	2
帧控制域	序列号域	地址域	命令帧标示符	命令帧负载	FCS

图 3-71 命令帧

在帧控制域中定义了帧的类型为命令帧，其地址域根据不同的命令存在两种长度，命令帧的具体功能由帧的负载数据表示。负载数据是一个变长结构，所有命令帧负载的第一个字节是命令类型字节，后面的数据针对不同的命令类型有不同的含义。在本节所建立的无线传感网中，用到的命令类型有关联请求（association request）、关联响应（Association response）、数据请求（Data request）等。

（4）确认帧：用以确认目标节点成功接收到数据帧或命令帧。当目标节点成功接收到数据帧或命令帧后，就发送一个确认帧给发送方。发送方接收到这个确认帧说明发送成功。若在规定的时间内没有接收到确认帧，则重发该数据帧或命令帧。确认帧的结构如图 3-72 所示。

字节：2	1	2
帧控制域	序列号域	FCS

图 3-72 确认帧

在帧控制域中定义了帧的类型为确认帧。确认帧的序列号要与被确认帧相同，并且负载长度为零。确认帧紧接着被确认帧发送，不需要使用 CSMA-CA 机制竞争信道。

在整个无线传感网中，采取的是普通节点定时读取其传感器上的光强数据，并将光强数据发送给中心节点。中心节点对接收到的数据进行处理后传送给相应的节点用以控制其上的指示灯。在中心节点上的数据处理流程如图 3-73所示。

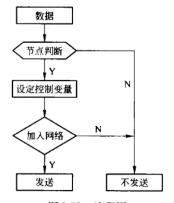


图 3-73 流程图

首先网络协调器对接收到的数据帧进行检验，图 3-73 中的“节点判断”是判断是否为指定节点的传感器数据。若接收的数据是指定节点上的数据，则将该数据与一个光

强度阈值进行比较来设定控制变量（用来控制灯的开关状态）。反之，则不进行发送操作。然后，判断带有指示灯的节点是否加入网络。若在网络中找到带有指示灯的节点，则中心节点将控制变量作为数据帧负载发送给它。反之则不发送带有控制变量的数据帧。

在我们设计的无线传感网中，普通节点将它采集的光强数据发送给网络协调器，网络协调器将含有控制变量的数据帧发送给带有指示灯接点的同时，还可以通过串口将光强度数据传送给计算机。通过安装在计算机上的监控软件，可以看出光强度信号的变化。如图 3-74 所示，通过遮盖光强传感器可以改变采集到的光强数据，当光强度比较低时曲线下降，反之曲线上升。从图 3-74 中可以明显看出，在这一段时间中传感器被遮盖了两次。

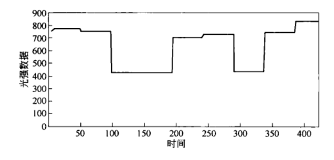


图 3-74　光强数据变化曲线图

设计实现了无线传感网，从无线传输协议的制定、传输过程控制等几个方面进行了论述。在实际运用中，只要对具体的传感器进行更换，就可以适用于各种各样的传感器网络。此系统适用于家庭、大厦内部环境质量的监控及智能化处理。由于无线传感器系统组网灵活，采用模块化的设计，故具有很好的移植性和扩展性，随着人们生活水平的提高，此系统在智能家电、家庭环境的智能调节上有着广阔的前景。

3.6　无线传感网高级关键技术——网络拓扑和路由协议

现有路由技术的局限性使其不能直接用于传感器网络，而针对移动网络设计的组网和通信协议一般也不适合于传感器网络。其重要原因之一是其扩展性的要求不同，移动网络相对节点的移动性来讲，扩展性问题并不十分突出；而传感器网络要求支持大规模网络，节点的移动性较弱甚至没有，主要问题变为如何延长网络的生存时间。这决定了两种网络有不同的优化目标。因此，有必要针对交通示范工程中交通信息数据采集、传输等特点，研究传感器网络路由协议，重点解决提高扩展性、低功耗、适应网络拓扑结构的变化等问题。

网络拓扑及路由是无线传感网中最重要的技术之一。在由无线传感网生成的网络拓扑中，可以直接通信的两个结点之间存在一条拓扑边。如果没有拓扑控制，所有结点都会以最大无线传输功率工作。在这种情况下，一方面，结点有限的能量将被通信部件快速消耗，降低了网络的生命周期。同时网络中每个结点的无线信号将覆盖大量其他结点，造成无线信号冲突频繁，影响结点的无线通信质量，降低网络的吞吐率。另一方面，在生成的网络拓扑中将存在大量的边，从而导致网络拓扑信息量大，路由计算复杂，浪费了宝贵的

计算资源。因此需要研究无线传感网中拓扑问题，在维持拓扑的某些全局性质的前提下，通过调整结点的发送功率来延长网络生命周期，提高网络吞吐量，降低网络干扰，节约结点资源。

3.6.1 无线传感网协议栈基本结构

无线传感网协议栈体系结构主要由物理层（PHY）、媒体接入层（MAC）、网络/安全层以及应用框架层组成，各层之间的分布如图3-75所示。

协议栈最底层网络层（PHY层）的特征是启动和关闭无线收发器，能量检测，链路质量，信道选择，清除信道评估（CCA）以及通过物理媒体对数据包进行发送和接收。MAC层可以实现信标管理、信道接入、时隙管理、发送确认帧、发送连接及断开连接请求，还为应用合适的安全机制提供一些方法。它包含具有时间同步信标可选超帧结构，采用免碰撞的载波侦听多址访问（CSMA-CA）。

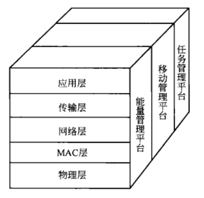


图3-75 体系结构

2000年12月，IEEE802无线个域网（Wireless Personal Area Network，WPAN）小组成立，致力于WPAN无线传输协议的建立。2003年12月，IEEE正式发布了该技术物理层和MAC层所采用的标准协议，即IEEE802.15.4协议标准，目前IEEE802.15.4已经成为无线传感网的物理层和媒体接入层的标准协议。

无线传感网安全层主要实现密钥管理、存取等功能。网络层主要用于ZigBee的LR-WPAN网的组网连接、数据管理等。应用框架层主要负责向用户提供简单的应用软件接口（API），包括应用子层支持APS（Application Sub-layer Support）、设备对象ZDO（ZigBee Device Object）等，实现应用层对设备的管理，为无线传感网技术的实际应用提供一些应用框架模型等，以便对ZigBee技术开发应用。

无线传感网网络层的定义包括网络拓扑、网络建立、网络维护、路由及路由的维护。

无线传感网有如下三种基本拓扑结构：

（1）星型拓扑结构（Star），主要为一个节点与多个节点的简单通信设计；

（2）树型拓扑结构（Tree），使用分等级的树型路由机制；

（3）网格型拓扑结构（Mesh），将Z-AODV和分等级的树型（Tree）路由相结合的混合路由方法。

三种拓扑结构如图3-76所示。

ZigBee定义了三种设备类型：ZigBee协调器（ZigBee Coordinator，ZC），用于初始化网络信息，每个网络只有一个ZC；ZigBee路由器（ZigBee Router，ZR），它起监视或控制作用，但它也是用跳频方式传递信息的路由器或中继器；ZigBee终端设备（ZigBee End Device，ZED），它只有监视或控制功能，不能做路由或中继之用。

在IEEE802.15.4标准中，ZED被称为精简功能设备（Reduced-Function Device，RFD），ZC和ZR被称作全功能设备（Full-Function Device，FFD）。

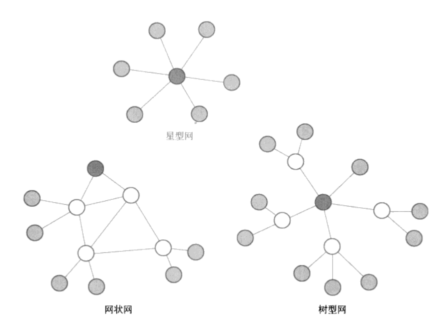


图 3-76　网络的三种拓扑结构

3.6.2　无线传感网路由基础

无线传感网是一种特殊 Ad hoc 网络（一个没有有线基础设施支持的移动网络），网络中节点密集，数量巨大且分布在十分广泛的区域。

目前发展前景最为看好的是基于 IEEE802.15.4 标准的 ZigBee 无线网络。无线传感网通常并不需要较高的传输带宽，但却需要较低的传输延时和极低的功率消耗，使用户能拥有较长的电池寿命和较多的器件阵列，而 ZigBee 的出现正好解决了这一问题。

ZigBee 是一个由多到 65000 个无线数传模块组成的无线数传网络平台，十分类似现有的移动通信 CDMA 网或 GSM 网，每一个 ZigBee 网络数传模块类似移动网络的一个基站，在整个网络范围内，它们之间可以进行相互通信。不同的是 ZigBee 网络主要为自动化控制数据传输而建立，每个 ZigBee 网络节点既可以与监控对象直接进行数据采集和监控，还可以自动中转其他网络节点传输的数据资料。除此之外，每个 ZigBee 网络节点还可在自己信号覆盖的范围内，与多个不承担网络信息中转任务的孤立子节点无线连接。

无线传感网中的节点大体可以分为两种类型：有路由容量的节点和没有路由容量的节点。对于树簇拓扑的无线传感网来说，终端设备通常是 RFD 精简设备，因此没有路由容量，而路由器与协调器是由 FFD 全功能设备组成的，因此有路由容量。

树簇型拓扑无线传感网中，通常采用树簇算法与 AODVjr 算法相结合的路由算法，其中树簇算法指的是消息沿着树型拓扑进行传输的算法，它是静态的，不需要存储路由表。该算法适用于节点静止或者移动较少的场合。而 AODVjr 算法则是对 Ad Hoc 按需距离矢量路由算法的改进，考虑到节能、应用方便性等因素，对 AODV 的一些特点进行了简化，但是仍然保留了 AODV 的原始功能。

这两种算法的结合使用确定了无线传感网路由的三种模式，即禁止路由模式、使能路由模式和强制路由模式。禁止路由模式就是禁止对路径进行查找，因此处于该模式的网络只能使用树簇算法沿着树型拓扑进行路由；使能路由模式是将树簇算法与 AODVjr 算法相结合，视具体情况来决定到底采用哪种路由算法；强制路由模式完全使用了 AODVjr 算法，只要设备具有路径查找能力，不管消息传输的路径是否已经存在，都要启动一个路径查找过程，当查找完成，数据包将沿着计算出来的路径传送。

路由的设定通常有三种模式，即禁止路由发现、使能路由发现及强制路由发现。

(1) 禁止路由发现（SUPPRESS）：如果发现网络路由器存在，数据包路由指向该路由器。否则，数据包沿着树型推进。

(2) 使能路由发现（ENABLE）：如果发现网络路由器存在，数据包路由指向该路由器。如果网络路由器不能确定，路由器可以启动一个路由发现过程，当发现完成，数据包将沿着计算出来的路由传送。如果该路由器没有路由发现能力，数据包将沿着树型推进。

(3) 强制路由发现（FORCE）：如果路由器有路由发现能力，不管路由是否已经存在，都将启动一个路由发现过程。发现完成，数据包将沿着计算出来的路由传送。如果这个路由器没有路由发现能力，数据包将沿着树型推进。这个选择必须小心使用，因为它会产生较大的网络冗余。它的主要用途是修复破坏了的路由。

对于树型拓扑结构设备间的数据转发，通常将源地址简化为上行路由（route up）或下行路由（route down）。如果 LocalAddr < DestAddr < LocalAddr + CSkip（d-1）为下行路由，否则为上行路由。通常网络的协调器或路由器都含有一个邻接设备表，该表记录了一定区域内与其具有邻接关系的设备。若想使用邻接表进行路由，只要目标设备在物理区域内可见，即可直接发送信息。而对于网状拓扑结构，则要使用路由表来进行路由。通常协调器或路由器都拥有自己的路由表，如果目标设备在路由表中有相关的记录，则信息就可以根据路由表中的记录进行发送，否则就要沿着树型拓扑来传输数据。

路由过程主要为以下几个步骤：

(1) 一个设备发出路由请求命令帧启动路由发现过程。

(2) 对应的接收设备收到该命令后，回复应答命令帧。

(3) 对潜在的各条路径花费（跳转次数、延迟时间）进行评估比较。

(4) 最佳路由记录添加到此路径上各个设备的路由表中。

通常路径请求与路径应答都是由路由器或协调器创建的。当路由器广播发送路径请求时，通常不会只发一次，而是间隔一段时间重复进行发送，而且对于广播寻址来说，它拥有两大特点：一个是凡有无线 RF 收发使能的设备皆能接收到该帧；另外就是广播发送采用一种被动应答模式，即当某一设备广播发送消息时，它还要监听所有的邻居设备是否对该帧进行广播转发，若没有则设备还要再次广播发送该帧。这样就会出现网络中的设备可能多次收到同一个路径请求，目的设备也有可能在一段时间内多次收到同一个路径请求。目的设备究竟应该响应哪个路径请求呢？在路径算法的实现中作者采用首接为最优的思想，即第一个收到的有效路径请求即为目的设备要响应的请求，在该请求中记录的路径即为消息传输的路径，应答命令将沿着收到的第一个路径请求命令帧中记录的上一级地址发送回去。

无线传感网可以采用多种网络路由算法，其中 Tree、Z-AODV、Tree + Z-AODV 等路由

算法是比较常见的算法。

3.6.3 AODV 路由协议

DSDV（destination-sequenced distance-vector）协议是一个基于传统的 BellmanFord 路由机制的表驱动算法，被认为是最早无线自组网络路由协议。DSDV 在传统 distance-vector 算法的基础上采用了序列号机制，用于区分路由的新旧程度，防止 distance-vector 算法可能产生的路由环路。DSDV 采用时间驱动和事件驱动技术控制路由表的传送，即每个移动节点在本地都保留一张路由表，其中包括所有有效目的节点、路由跳数、目的节点路由序列号等信息，目的节点路由序列号用于区别有效和过期的路由信息以避免环路的产生。

DSR（dynamic source routing）协议是最早采用按需路由思想的路由协议，包括路由发现和维护两个过程。它的主要特点是使用了源路由机制进行数据包转发。

AODV（Ad hoc on-demand distance vector）协议在 DSDV 协议的逐跳路由、序列号、定期广播机制基础上，加入了 DSR 的按需路由发现和维护机制。

AODV 在每个中间节点隐式保存了路由请求和应答的结果，并利用扩展环搜索（expanding ring research）的办法限制搜索发现目的节点的范围。AODV 支持组播功能，支持 QoS，而且 AODV 使用 IP 地址，便于同 Internet 连接。但 AODV 基于双向信道的假设，路由应答数据包直接沿着路由请求的反方向回溯到源节点，因而不支持单向信道。与 DSDV 保存完整的路由表不同的是，AODV 通过建立按需路由来减少路由广播的次数，这是 AODV 对 DSDV 的重要改进。与 DSR 相比，AODV 的好处在于源路由并不需要包括在每一个数据包中，这样会降低路由协议的开销。AODV 是一个纯粹的按需路由协议，那些不在路径内的节点不保存路由信息，也不参与路由表的交换。

3.6.3.1 DSDV 和 AODV 的比较

（1）在网络中的每一个变化，DSDV 都向每个节点发广播。在 AODV 中则不需要发送这种广播。

（2）当两个邻居节点进出彼此的通信范围时，这就造成了广泛的网络广播。如果一个链接破损不影响正在进行的传输就不会发生全球性的广播，仅仅受影响的节点被通知。

（3）局部的活动会造成全局的影响；节点的局部运动只对局部产生影响，AODV 降低了网络在大范围内广播的可能，与 DSDV 相比，在控制开销上有显著的减少。

3.6.3.2 AODV 的特性

AODV 具有如下特性：

（1）AODV 按照需要发现路线。不保留从任意节点到其他节点的路线。

（2）只有需要的路线才会长期保留。

（3）每个节点单调地保留其不断增长的序列号，每次节点在邻里拓扑中发现有变化，序列号就会增加。

（4）AODV 按照路由表来存储路由信息：一个针对单播路由的路由表和一个针对组播路由的路由表。

（5）路由表存储：<目的地址、下一跳地址、目的地序列号、生命周期>。

(6) 针对每个目的地，一个节点保留一个前驱节点列表。

(7) 每次路由使用都会更新生命周期，如果路由没用到生命周期，则表示其到期了。

3.6.3.3 AODV 路由发现

(1) 如果某个节点希望发送一个数据包到某个目的地，它会检测路由表确定是否存在一条到达目的地的现成的路线。如果存在，转发数据包到下一条节点；如果不存在，它将启动一个路由发现过程。

(2) 路由发现过程开始于创建一个路由请求（RREQ）包，它由源节点创建。这个包包括源节点 IP 地址、源节点当前序列号、目的地 IP 地址、目的地序列号。

(3) 数据包同样包括广播编号：每次源节点使用 RREQ，广播编号随之递增；广播编号和源 IP 地址构成具有独特标志符的 RREQ。

3.6.3.4 控制包传送

(1) 发送点 S 向其所有邻居节点广播一个控制包 P。

(2) 每个节点接收到 P，然后再将 P 向前发送给它的邻居节点。

(3) 序列号避免了多次发送统一控制包的可能性。

(4) 包 P 到达目的地 D，假如发送点 S 可以到达 D。

(5) 节点 D 不能再向前发送。

3.6.3.5 控制包传送例子

控制包传送的例子如图 3-77 ~ 图 3-84 所示。

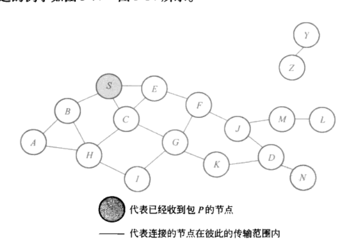


图 3-77 控制包传送 1

节点 H 收到了来自两个邻居节点的包 P：潜在的碰撞。

节点 C 收到来自节点 G 和 H 的包 P，但是不会再转发包 P，因为节点 C 已经转发过一次包 P 了。

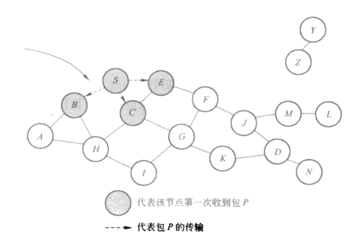


图 3-78　控制包传送 2

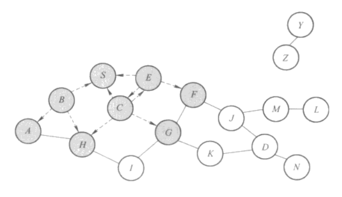


图 3-79　控制包传送 3

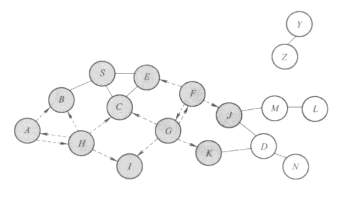


图 3-80　控制包传送 4

节点 J 和 K 都向节点 D 广播包 P。

由于节点 J 和 K 是彼此隐藏的，它们的传输可能发生碰撞。

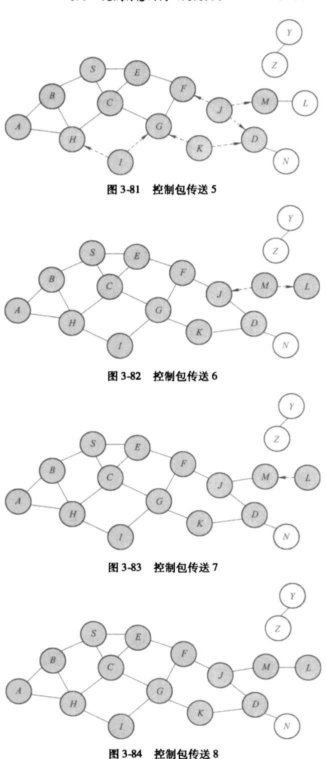


图 3-81 控制包传送 5

图 3-82 控制包传送 6

图 3-83 控制包传送 7

图 3-84 控制包传送 8

节点 D 不会转发包 P，因为节点 D 是包 P 的目的地。

Flooding 结束。

从节点 S 不能到达的节点不能收到包 P（例如节点 Z）。

要通过目的节点 D 才能到达的节点也不能接收到包 P（例如节点 N）。

Flooding 可能将包 P 传送给太多的节点（最坏的情况，所有从源节点能到达的节点都可能接收到了包）。

3.6.3.6　路由发现

（1）一旦一个中间节点接收到了路由请求（RREQ），该节点就在其路由表中为源节点建立一个反向路由入口。反向路由入口包括 < 源 IP 地址、源序列号、到源节点的跳数、收到 RREQ 的节点 IP 地址 >，通过反向路由，节点可以向源节点发送一个 RREP（路由应答包）。

（2）RREQ 到达目的地。为了对 RREQ 做出应答，该节点必须位于其路由表中：

1）对于目的点来说为过期的入口。

2）序列号至少要同目的点的一样大（为了预防环路）。

（3）RREQ 到达目的地（续）：

1）如果两个条件满足，同时目的地的 IP 地址和 RREQ 中的相吻合，那么该节点就用单播和非 FLOODING 方式利用反向路径向源节点发送一个 RREP 回去，以对 RREQ 做出应答。

2）如果不满足条件，节点就增加 RREQ 中的跳变数，同时向其邻居节点发广播。

3.6.3.7　路由发现例子

路由发现的例子如图 3-85 ~ 图 3-91 所示。

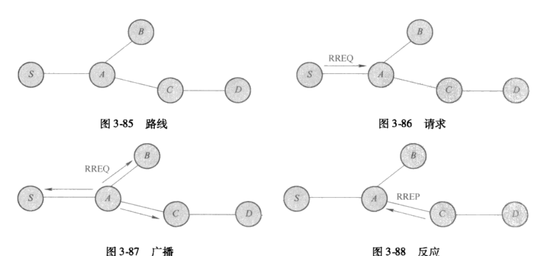


图 3-85　路线　　图 3-86　请求

图 3-87　广播　　图 3-88　反应

（1）S 节点需要一条到达节点 D 的路线，如图 3-85 所示。

（2）创建一个路由请求（RREQ），装入节点 D 的 IP 地址、序列号、S 点的 IP 地址、

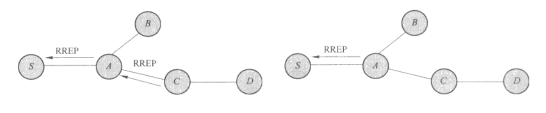


图 3-89 C 创建一个路由应答包 图 3-90 A 发 RREP

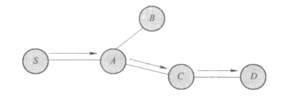


图 3-91 创建一个到 D 的前向路径入口

系列号、跳变数（=0），如图 3-86 所示。

（3）节点 S 向其邻居节点广播 RREQ。

（4）节点 A 收到 RREQ。为节点 S 建立一个反向路由入口（dest = S，下一跳 = S，跳变数 = 1）。

（5）A 没有路线到 D，所以它重播 RREQ。

（6）节点 C 收到 RREQ。为节点 S 建立一个反向路由入口（dest = S，下一跳 = A，跳变数 = 2）。

（7）C 有路线到 D，在 RREQ 中，到 D 的路由序列号大于等于 D 的序列号。

（8）C 创建一个路由应答包（RREP），装入 D 的 IP 地址、序列号、S 的 IP 地址、到 D 的跳变数（=1），同时向 A 单播 RREP。

（9）A 收到 RREP。创建一个到 D 的前向路径入口（deat = D，下一跳 = C，跳变数 = 2）同时单播 RREP 到 S。

（10）S 收到 RREP。创建一个到 D 的前向路径入口，（dest = D，下一跳 = A，跳变数 = 3）。

（11）在线路上向 D 发送数据包。

3.6.3.8 在 AODV 中的路线请求

在 AODV 中的路线请求如图 3-92 ~ 图 3-97 所示。

C 节点收到来自 G 和 H 的 RREQ，但是不会再向前发送了，因为节点 C 已经发送过一次 RREQ 了。

节点 D 不会向前发送 RREQ 了，因为它是 RREQ 中定义的目标节点。

当 RREP 沿着反向路径传输时，前向路径就被建立了。

路由表入口用来向前传输数据包。路径并没包括在包头里。

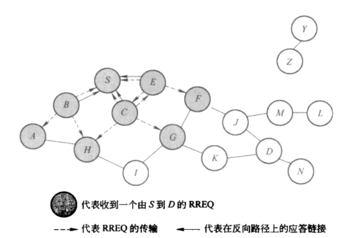


图 3-92 路线请求 1

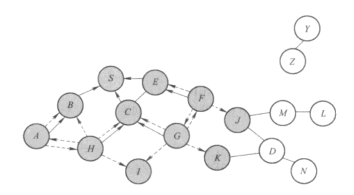


图 3-93 路线请求 2

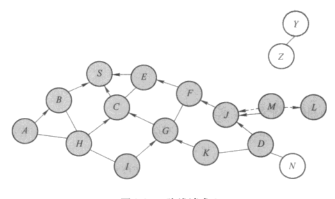


图 3-94 路线请求 3

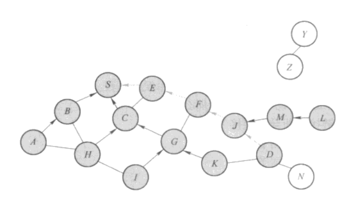


图 3-95 路线请求 4

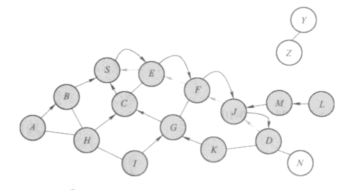


图 3-96 路线请求 5

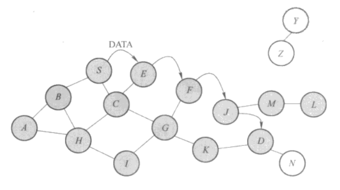


图 3-97 路线请求 6

3.6.3.9 链接故障报告

（1）节点 X 的邻居节点被优先考虑为路由表条目，如果邻居节点在优先路由超时间隙内发送了一个包并且使用那个条目向前发送。

（2）如果源节点移动了，将会重新启动路由发现过程。

（3）如果中间或者目的节点移动，那么：

1）下一跳的链接中断导致链接失败。

2）为链接失败更新路由表。

3）通知所有活动的邻居节点。

3.6.3.10 路由维护 RERR

（1）中断的上游节点（更靠近源节）将启动 RERR。

1）它将传播到所有受影响的目的节点。

2）RERR 将列出所有受到链接失败影响的节点，即当时正在使用链接传送信息的那些节点。

3）当节点收到 RERR 时，它将标记它到目的节点的路径为无效，即在路由表中设置到达目标节点的距离为无限远。

（2）当源节点收到 RERR，它就可以重启路由发现。

3.6.3.11 路由维护例子

路由维护例子如图 3-98 ~ 图 3-100 所示。

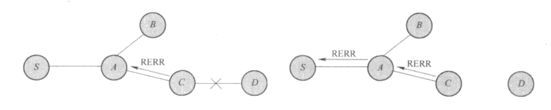


图 3-98 路由维护 1　　　图 3-99 路由维护 2

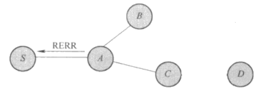


图 3-100 路由维护 3

（1）C 和 D 之间连接发生中断。

（2）节点 C 在路由表中让到 D 的路线无效。

（3）节点 C 创建路线错误消息。

1）列出目前所有未能到达的目标节点。

2）发送给上游邻居节点。

（4）节点 A 收到 RERR。

1）检查在路由上节点 C 的小一跳是不是节点 D。

2）删除到 D 的路径。

3）向前发送 RERR 给节点 S。

（5）节点 S 收到 RERR。

1）检查在路由上节点 A 的下一条是否是节点 D。

2）删除到 D 的路径。

3）如果仍然需要，则重新发现路径。

3.6.3.12 路由错误

（1）当节点 X 不能够在链接（X，Y）向前传送包 P（从节点 S 到节点 D）的时候，它将产生一个错误消息。

（2）节点 X 将增加为节点 D 设置的缓存在节点 X 的序列号。

（3）增加的序列号 N 将包含在 RERR 中。

（4）当源节点 S 收到 RERR 时，它将为 D 设置至少比 N 大的序列号来启动路由发现。

3.6.3.13 链接失败检测

（1）问候信息：邻居节点之间周期性地交换问候信息。

（2）丢失问候信息就被作为链接失败的指示。

（3）另外，接受 MAC 层确认多次失败也可以认为是链接失败。

3.6.3.14 序列号在 AODV 中作用

（1）避免使用过时/中断的路由——用于检测的路由是新的。

（2）为了防止环路产生，如图 3-101 所示。

1）最初节点 A 有条到 D 的路径。

2）假设节点 A 不知道 C—D 之间的链接失败，因为从 C 发送的 RERR 丢失了。

3）现在 C 为 D 执行一条路由发现，节点 A 收到 RREQ（经 C—E—A），节点 A 将回复，因为 A 认为到达节点的路径是通过节点 B。

4）导致环路的产生（例如，C—E—A—B—C），如图 3-102 所示。

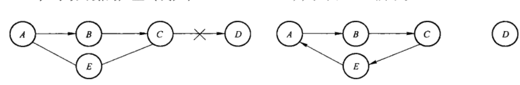


图 3-101 环路产生 1　　图 3-102 环路产生 2

5）但是由于使用序列号，节点 A 将不会使用路径 A—B—C，因为这条路径的序列号要比节点 A 从它自身收到的序列号要小。

3.6.4 Z-AODV 能量平衡路由算法

在 ZigBee 路由规范中没有过多地考虑能量控制，但是对于 Ad hoc 无线网络来说，能量控制非常重要，因此提出了能量控制策略来改进 ZigBee 路由。它将使节点避免用尽所有能量以至于过早地失去作用。当节点想要选择路径时，它将考虑路径上的节点的剩余能量。

Z-AODV 算法是针对 AODV（Ad hoc 按需距离矢量路由协议）算法的改进，AODV 是基于序列号的路由，它总是选择最新的路由。Z-AODV 基于路径的能量消耗的路由，考虑了节能、应用方便性等因素，简化了 AODV 的一些特点，但仍保持 AODV 的原始功能。

在路由选择和路由维护时，ZigBee 的路由算法使用了路由成本的度量方法来比较路由的好坏。假定一个长度为 L 的路由 P，则它的路由成本为：

$$C(p) = \sum_{i=1}^{L=1} C\{[D_i, D_{i+1}]\}$$

式中，$C\{[D_i, D_{i+1}]\}$ 表示从节点 D_i 到节点 D_{i+1} 的链路成本，对于链路 1，链路成本可按照下面的表达式计算：

$$C\{l\} = \begin{cases} 7 \\ \min\left(7, \text{round}\left(\frac{1}{p_1^4}\right)\right) \end{cases}$$

其中，p_1 为链路中发送数据包的概率。

在 ZigBee 规范中没有涉及 p_1 的具体计算方法。p_1 可通过实际计算收到的信标和数据帧来进行估计，即通过观察帧的响应序列号来检测丢失的帧，这就是通常被认为最准确地测量接收概率的方法。但是，对于所有的方法来说，最直接和有效的方法就是基于 IEEE802.15.4 的 MAC 层和 PHY 层所提供的每一帧的 *LQI* 通过平均所计算的值。即使使用其他方法，最初的成本估计值也是基于平均的 *LQI* 值。可以根据驱动函数表来映射平均 *LQI* 值与 C {l} 值的关系（见表 3-6）。

表 3-6 *LQI* 值与链路成本的关系

LQI	链路成本	*LQI*	链路成本
>75	1	<50	7
50～75	3		

能量平衡运算要考虑许多因素来选择路由。这些因素包括临近节点的能量、节点自身的能量和链路质量。剩余能量 Elocal 可以在每一个 ZigBee 帧中的保留域发送，这样每个节点都能得到它的邻居节点最新的能量分配 {E1，E2，…，En}。

3.6.5 树型（Tree）路由算法

树型路由机制包括配置树型地址和树型地址的路由。当协调器建立一个新的网络，它将给自己分配网络地址 0，网络深度 Depth0 = 0。如果节点 i 想要加入网络，并且与节点 k 连接，那么节点 k 将称为节点 i 的父节点。根据自身的地址 Ak 和网络深度 Depthk，节点 k

将为节点 i 分配网络地址 Ai 和网络深度 Depthi = Depthk + 1。网络深度表示仅仅采用父子关系的网络中，一个传送帧传送到 ZigBee 协调器所传递的最小跳数。ZigBee 协调器自身深度为 0，而它的子设备深度为 1。

ZigBee 树型结构，参数 nwkMaxChildren（Cm）表示路由器或协调器在网络中允许拥有子设备数量的最大值。参数 nwkMaxRouters（Rm）表示子节点中路由器的最大个数，而剩下的设备数为终端设备数。

一个新的 RFD 节点 i，它没有路由能力，它与协调器连接作为协调器的第 n 个子节点。根据它的深度 d，父节点 k 将为子节点 i 分配网络地址：

$$A_i = A_k + C_{skip}(d) \cdot R_m + n$$

其中，$1 \leq n \leq C_m - R_m$。

如果是新的子节点 FFD，它有路由能力，父节点（k）将给它分配网络地址：

$$A_i = A_k + 1 + C_{skip}(d) \cdot (n - 1)$$

式中

$$C_{skip} = \begin{cases} 1 + C_m(L_m - d - 1), 如果 R_m = 1 \\ \dfrac{1 + C_m - R_m - C_m \cdot R_m{}^{L_m - d - 1}}{1 - R_m} \end{cases}$$

否则，参数 nwkMaxDepth（L_m）表示网络的最大深度。

假设一个路由器向网络地址为 D 的目的地址发送数据包，路由器的网络地址为 A，网络深度为 d。路由器将首先通过表达式：

$$A < D < A + C_{skip}(d - 1)$$

判断该目的节点是否为自己的子节点。如果目的节点是自己的子节点，则下一跳节点的地址为：

$$N = \begin{cases} D, 如果是终端设备 \\ A + 1 + \left[\dfrac{D - (A + 1)}{C_{skip}(d)}\right] \times C_{skip}(d) \end{cases}$$

否则，下一跳节点是该路由器的父节点。

3.6.6 Tree + Z-AODV 路由算法

根据前面对 Tree 和 Z-AODV（也称为 AODVjr）两种路由算法的介绍，Cluster-Tree（簇-树）是一种由网络协调器（Coordinator）展开生成树状网络的拓扑结构，适合于节点静止或者移动较少的场合，属于静态路由，不需要存储路由表。AODVjr 算法是针对 AODV（Ad hoc 按需距离矢量路由协议）算法的改进，考虑到节能、应用方便性等因素，简化了 AODV 的一些特点，但是仍然保持 AODV 的原始功能。表 3-7 所示是两种算法优缺点比较。

表 3-7 两种算法比较

优缺点	Cluster-Tree	AODVjr
优 点	简单，无初始延迟	路径最佳，自适应
缺 点	路由非最佳，非自适应	需要路由表，有初始延迟

如果将两者结合，使用 Z-AODV 和分等级的树型（Tree）路由相结合的混合路由方法，构成的网格型拓扑结构（Mesh）的网络。Cluster-Tree + AODVjr 路由算法汇聚了 Cluster-Tree 算法和 AODVjr 算法的优点。

网络中的每个节点被分成四种类型：Coordinator、RN +、RN -、RFD（RN：Routing Node，路由节点；RFD：Reduced Function Device）。

其中 Coordinator 的路由算法跟 RN + 相同，Coordinator、RN + 和 RN - 都是全功能节点（FFD：Full Function Device），能给其他节点充当路由节点；RFD 只能充当 Cluster-Tree 的叶子（Leaf Node）。如果待发送数据的目标节点是自己的邻居，直接通信即可；反之，如果不是自己的邻居时，三种类型的节点处理数据包各不相同：RN + 可以启动 AODVjr，主动查找到目标节点的最佳路由，且它可以扮演路由代理（Routing Agent）的角色，帮助其他节点查找路由；RN-只能使用 Cluster-Tree 算法，它可以通过计算，判断该数据包来自自己的父节点还是某子节点转发；而 RFD 只能把数据交给父节点，请其转发。

图 3-103 所示为 Cluster-Tree + AODVjr 算法时网络层数据传输示意图。节点 *E* 发送数据包给节点 *D*，数字代表各种包发送的时间先后次序。从图中可以看出，节点 *E* 的类型是 RFD，它只能将数据 DATA 传送给其父节点 *C*。*C* 的类型是 RN +，所以它先把数据放入缓存后，再通过组播 AODVjr 路由请求包 RREQ 查找到节点 *D* 的路由，节点 *D* 再通过单播沿最短的路径 *D*—*B*—*C* 给节点 *C* 回复 AODVjr 路由应答包 RREP。节点 *C* 找到路由后，把缓存数据沿 *C*—*B*—*D* 发送给节点 *D*，节点 *D* 再沿 *D*—*B*—*C*—*E* 发送确认包 *ACK* 给节点 *E*，节点 *E* 收到确认包后，整个通信过程结束。

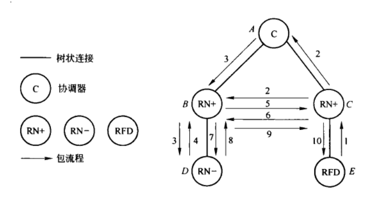


图 3-103　数据传输示意图

1，6，7—数据包（DATA）；2，3—路由请求包（RREQ）；
4，5—路由应答包（RREP）8，9，10—确认包（ACX）

具体实现方法是在数据帧帧头的 DiscoverRouter 域指定路由。该域可以是如下三种值：

（1）抑制路由发现。它使用已经存在的路由表。当路由表中没有相应的目的节点的地址时，参数 nwkUseTreeRouting 的值为 TRUE，网络将使用树型路由。

（2）使能路由发现。如果在路由表中有路由地址，将按照该路由表进行路由。否则，

路由器将使用Z-AODV路由算法初始路由发现。如果该节点没有初始路由发现的能力，它将使用树型路由。

（3）强制路由发现。不管是否有相应的路由表，节点都强制使用Z-AODV路由算法初始化路由发现。

在ZigBee规范中提出了将AODV和Tree路由混合的路由机制。但在ZigBee规范中并没有说明如何配置参数来选择路由策略，没有使两者平衡的设计方法。根据上面Tree路由和Z-AODV的分析，我们提出了基于数据特性的路由方法，即在两种路由算法构成的网格形网络中，根据节点间传输数据特性的不同，通过设置数据帧帧头DiscoverRouter域，选择不同的路由方法。

对于捆绑型的连续数据，ZigBee应用层应选择使用使能路由的方法。即采用Z-AODV路由首先建立路由发现，然后选择跳数少的路由，成为最佳路径；对于爆发型的不连续数据则使用抑制路由发现的方法，即在路由表中没有响应的目的节点的地址时，采用Tree路由方法。因为这种路由不需要建立路由表，因此对传输的数据响应较快。

图3-104所示为节点接收到上层或其他节点发送的数据包时，网络层处理程序的流程图。

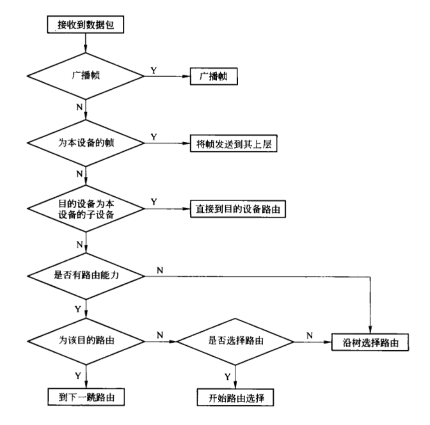


图3-104 路由算法流程图

Tree 路由是一种由网络协调器展开生成树状网络的拓扑结构，适合于节点静止或者移动较少的场合，属于静态路由，不需要存储路由表。树型路由对传输数据包的响应较快，因为树型路由不需要建立路由表。其缺点是所选择的路由并非是最佳的路由，不能获得最小路由。树型路由适用于爆发型的数据传输。

Z-AODV 需要首先建立路由发现，然后选择跳数少的路由，成为最佳路径。Z-AODV 适用于连续的数据传输。

在 ZigBee 规范中，设计了 Z-AODV 和 Tree 路由混合的路由策略，这里我们提出了基于数据服务的 ZigBee 路由选择策略。根据上述分析可以看出，这种路由选择机制在网络性能和低功耗方面有明显的优势；并且根据能量控制机制，可以有效地平衡节点能量，避免节点耗尽能量而过早地失去作用。

3.6.7 无线传感网络路由设置实验

下面介绍基于无线传感器网络平台 EXPLORERF-MC13224 或 DREAMRF-MC13224 的无线传感器网络路由设置实验。

ZigBee 中设备最大数量由网络允许情况决定，ZigBee 决定最大数量的路由器，最大数量的终端节点。一个 ZigBee 无线网络必须至少包括 1 个协调器。

协调器是网络的发起者，它的网络深度为 0。协调器的子节点网络深度为 1，再向下一级设备网络深度增加 1。网络最大负载量由网络最大深度与每一个路由器允许的最大子设备数量决定。

例如，图 3-105 中节点 8（Node 8）网络深度（Depth）为 1，节点 9 网络深度为 2，节点 3 网络深度也为 2。

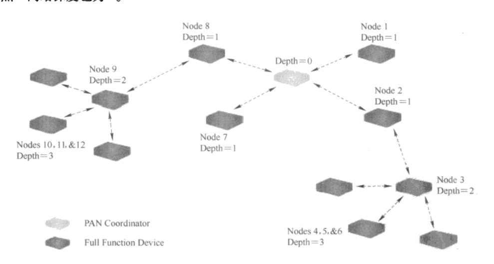


图 3-105 网络深度显示图

最大数量的子节点数是指允许连接到父节点设备的最大的设备数量。

在“BeeStackConfiguration. h”文件中设置相关网络参数，如图 3-106 所示。

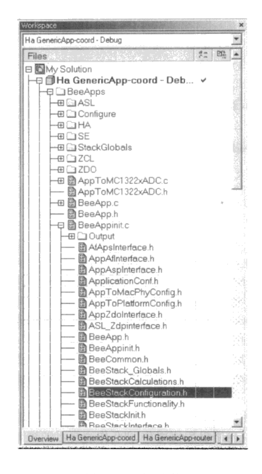


图 3-106　设置文件

```
/*
  Maximum children each router(including ZC) can keep track of. To determine number of end-devices, subtract MaxRouters.
  Default 20(0x14) in stack profile 1
*/
#ifndef gNwkMaximumChildren_c
#define gNwkMaximumChildren_c    20
#endif
```

gNwkMaximumChildren_c 设置每个路由器可连接节点最大个数（包括路由器及终端设备）。

```
/*
  Maximum depth from the ZigBee Coordinator(ZC) in number of hops. This also
  limits the default network diameter to 2 * maxDepth.
```

```
  Default 15 in stack profile 2
 */
#ifndef gNwkMaximumDepth_c
#define gNwkMaximumDepth_c          5
#endif
```

gNwkMaximumDepth_c 设置 ZigBee 无线网络的最大网络深度。

```
/*
  Maximum number of routers each router(including ZC)can keep track of.
  Default 6 in Stack Profile 1
 */
#ifndef gNwkMaximumRouters_c
#define gNwkMaximumRouters_c        6
#endif
```

gNwkMaximumRouters_c 设置路由器可连接路由器最大个数。

ZigBee 有两种地址分配方式：分布式分配机制和随机分配机制。

（1）随机分配机制。随机分配机制是指当 NIB 的 nwkAddrAlloc 值为 0x02 时，地址随机选择。在这种情况下 nwkMaxRouter 就无意义了。随机地址分配应符合 NIST 测试中的描述。当一个设备加入网络使用的是 Mac 地址，其父设备应选择一个尚未分配过的随机地址。一旦设备已分配一个地址，它没有理由放弃该地址，并应予以保留，除非它收到声明，其地址与另一个设备冲突。此外，设备可能自我指派随机地址，比如利用加入命令帧加入一个网络。

（2）分布式分配机制。我们知道，每个 ZigBee 设备应该拥有一个唯一物理地址。协调器（coordinator）在建立网络以后使用 0x0000 作为自己的短地址。在路由器（router）和终端（enddevice）加入网络以后，使用父设备给它分配的 16 位的短地址来通讯。那么这些短地址是如何分配的呢?

16 位的地址意味着可以分配给 65536 个节点之多，地址的分配取决于整个网络的架构，整个网络的架构由这 3 个值决定：

1）网络的最大深度（L_m）；

2）每个父亲设备拥有的孩子数（C_m）；

3）第 2 条的孩子设备当中有几个是路由器（R_m）。

有了这 3 个值就可以根据下面的公式来算出某父设备的路由器与子设备之间的地址间隔 $C_{skip}(d)$：

$$C_{skip(d)} = \begin{cases} 1 + C_m(L_m - d - 1), \text{ if } R_m = 1 \\ \dfrac{1 + C_m - R_m - C_m \times R_m^{L_m - d - 1}}{1 - R_m} \end{cases}$$

上面这个公式是用来计算位于深度 d 的父设备的，它所分配的子路由器之间的短地址间隔。该父亲设备分配的第 1 个路由器地址 = 父亲设备地址 + 1，分配的第 2 个路由器地址 = 父亲设备地址 + 1 + $C_{skip}(d)$，第 3 个路由器地址 = 父亲设备地址 + 1 + 2 × $C_{skip}(d)$，依

次类推。计算终端地址：

$$A_n = A_{\text{parent}} + C_{\text{skip}}(d) \times R_m + n$$

这个公式是用来计算 A_{parent} 这个父亲设备分配的第 n 个终端设备的地址 A_n 的。

举个简单的例子，假设有一个 ZigBee 网络，最大深度为 3，每个父亲的最大孩子数是 5，在孩子当中路由器数量是 3，如图 3-107 所示。

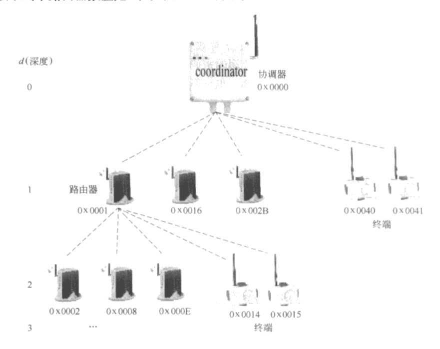


图 3-107 网络地址分配

由图 3-107 可知，协调器 $C_{\text{skip}}(d) = (1+5-3-5\times3^{3-0-1})/(1-3) = 21$，所以协调器第一个路由器是 1，第二个就是 22，换算成十六进制就是 0x0016。协调器第 1 个终端地址 = 0x0000 + 21 × 3 + 1 = 64 = 0x0040、第 2 个就是 0x0041。由此可见所有同一父亲终端设备的短地址都是连续的。

不难看出一旦 L_m、C_m、R_m 这 3 个值确定了，整个网络设备地址也就确定下来了。所以知道了某个设备短地址就可以计算出它的设备类型和它的父设备地址。

3.7 无线传感网高级关键技术——网络加密和安全

在无线传感网中，最小的资源消耗和最大的安全性能之间存在矛盾，这是传感器网络安全性的首要问题。通常两者之间的平衡需要考虑到有限的能量、有限的存储空间、有限的计算能力、有限的通信带宽和通信距离这五个方面的问题。

无线传感网在空间上的开放性，使得攻击者可以很容易地窃听、拦截、篡改、重播数据包。网络中的节点能量有限，使得无线传感网易受到资源消耗型攻击。而且由于节点部署区域的特殊性，攻击者可能捕获节点并对节点本身进行破坏或破解。

另外无线传感网是以数据通信为中心的，将相邻节点采集到的相同或相近的数据发送至基站前要进行数据融合，中间节点要能访问数据包的内容，因此不适合使用传统端到端的安全机制。

3.7.1 攻击及防御

由于传感器网络自身的一些特性，使其在各个协议层都容易遭受到各种形式的攻击。下面着重分析对网络传输底层的攻击形式。

物理层中安全的主要问题就是如何建立有效的数据加密机制。由于传感器节点的限制，其有限计算能力和存储空间使基于公钥的密码体制难以应用于无线传感网中。为了节省传感器网络的能量开销和提供整体性能，也尽量要采用轻量级的对称加密算法。

对称加密算法在无线传感网中的负载，在多种嵌入式平台构架上分别测试了 RC4、RC5 和 IDEA 等 5 种常用的对称加密算法的计算开销。测试表明在无线传感器平台上性能最优的对称加密算法是 RC4，而不是目前传感器网络中所使用的 RC5。

由于对称加密算法的局限性，不能方便地进行数字签名和身份认证，给无线传感网安全机制的设计带来了极大的困难。因此高效公钥算法是无线传感网安全亟待解决的问题。

数据链路层或介质访问控制层为邻居节点提供可靠的通信通道，在 MAC 协议中，节点通过监测邻居节点是否发送数据来确定自身是否能访问通信信道。这种载波监听方式特别容易遭到拒绝服务攻击也就是 DOS。在某些 MAC 层协议中使用载波监听的方法来与相邻节点协调使用信道。

当发生信道冲突时，节点使用二进制值指数倒退算法来确定重新发送数据的时机，攻击者只需要产生一个字节的冲突就可以破坏整个数据包发送。因为只要部分数据的冲突就会导致接收者对数据包校验和不匹配。导致接收者会发送数据冲突的应答控制信息 ACK 使发送节点根据二进制指数倒退算法重新选择发送时机。这样经过反复冲突，使节点不断倒退，从而导致信道阻塞。恶意节点有计划地重复占用信道比长期阻塞信道要花更少的能量，而且相对于节点载波监听开销，攻击者所消耗能量非常地小，对于能量有限节点，这种攻击能很快耗尽节点有限能量。所以，载波冲突是一种有效的 DOS 攻击方法。

虽然纠错码提供了消息容错的机制，但是纠错码只能处理信道偶然错误，而一个恶意节点可以破坏比纠错码所能恢复的错误更多的信息。纠错码本身也导致了额外的处理和通信开销。目前来看，这种利用载波冲突对 DOS 的攻击还没有有效的防范方法。

解决的方法就是对 MAC 的准入控制进行限速，网络自动忽略过多的请求，从而不必对于每个请求都应答，节省了通信的开销。但是采用时分多路算法的 MAC 协议通常系统开销比较大，不利于传感器节点节省能量。

通常，在无线传感网中，大量的传感器节点密集地分布在一个区域里，消息可能需要经过若干节点才能到达目的地，而且由于传感器网络动态性，因此没有固定的基础结构，所以每个节点都需要具有路由的功能。由于每个节点都是潜在的路由节点，因此更易于受到攻击。无线传感网的主要攻击种类较多，简单介绍如下：

（1）虚假路由信息。通过欺骗，更改和重发路由信息，攻击者可以创建路由环，吸引或者拒绝网络信息流通量，延长或者缩短路由路径，形成虚假的错误消息，分割网络，增加端到端的时延。

（2）选择性的转发。节点收到数据包后，有选择地转发或者根本不转发收到的数据包，导致数据包不能到达目的地。

（3）污水池（sinkhole）攻击。攻击者通过声称自己电源充足、性能可靠而且高效，通过使泄密节点在路由算法上对周围节点具有特别的吸引力吸引周围的节点选择它作为路由路径中的点。引诱该区域的几乎所有的数据流通过该泄密节点。

（4）Sybil 攻击。在这种攻击中，单个节点以多个身份出现在网络中的其他节点面前，使之具有更高概率被其他节点选作路由路径中的节点，然后和其他攻击方法结合使用，达到攻击的目的。它降低具有容错功能的路由方案的容错效果，并对地理路由协议产生重大威胁。

（5）蠕虫洞（wormholes）攻击。攻击者通过低延时链路将某个网络分区中的消息发往网络的另一分区重放。常见的形式是两个恶意节点相互串通，合谋进行攻击。

（6）Hello 洪泛攻击。很多路由协议需要传感器节点定时地发送 HELLO 包，以声明自己是其他节点的邻居节点。而收到该 Hello 包的节点则会假定自身处于发送者正常无线传输范围内。而事实上，该节点离恶意节点距离较远，以普通的发射功率传输的数据包根本到不了目的地。网络层路由协议为整个无线传感网提供了关键的路由服务，如受到攻击后果非常严重。

传输层用于建立 WSN 与 Internet 或者其他外部网络的端到端的连接。目前在 WSN 大多数应用中，都没有对于传输层的需求，传输层协议一般采用传统网络协议。

应用层提供了 WSN 的各种实际应用，因此也面临各种安全问题。密钥管理和安全组播为整个 WSN 的安全机制提供了安全支撑。

WSN 中采用对称加密算法、低能耗的认证机制和 hash 函数。目前普遍认为可行的密钥分配方案是预分配，即在节点部署之前，将密钥预先配置在节点中。实现方法有如下多种：

（1）基于密钥池的预配置方案。每个节点在部署前，从事先生成的密钥池中随机选取一定数目的密钥子集，节点部署到指定区域后，只与具有相同密钥的节点通信。

（2）基于多项式的预配置方案。由 C Blundo 等人提出，能有效地抵御节点被捕获，扩展性强，但计算开销大，也不支持邻居节点的身份认证。

（3）利用节点部署信息的预配置方案。节点按照地理位置关系分组给处于相同组或是相邻组的节点之间分配共享密钥，使节点的分组模式和查询更符合节点广播特征，提高密钥利用率，减少密钥分配和维护代价。

作为一种新的信息获取和处理技术，WSN 在某些领域有着传统技术不可比拟的优势，但由于传感器网络和节点自身的一些限制，给它的安全性设计带来了新的挑战。高效加密算法、安全的 MAC 协议和路由协议以及密钥管理和安全组播等都是值得深入研究的领域。

3.7.2 加密算法

无线传感网加密算法有 6 个，即 RC5、RC6、Rijndael、MISTY1、KASUMI 和 Camellia。这 6 个加密算法均有较好的安全件，目前没有对其有效的攻击，如表 3-8 所示。

表 3-8 加密算法比较

加密算法	密钥长度/位	轮 数	加密段长度/位
RC5-32	128	18	64
RC6-32	128	20	128
Rijndael	128	10	128
MISTY1	128	8	64
KASUMI	128	8	64
Camellia	128	18	128

除了 RC5，每种加密算法的加密轮数都采用标准轮数。根据相关技术报告中分析的安全问题，对 RC5 采用 18 轮加密代替原来的 16 轮。RC5 和 RC6 支持不同的加密段长度，但在没有相关理论支持的情况下，如果用 16 位的字长加密，就不知道 RC5、RC6 到底加密多少轮才算是安全的，所以对 RC5、RC6 采用标准 32 位加密字长。

把长的明文分成多个段，然后分别加密的方法叫做电子密码本模式，但这种模式可以通过对原始密文进行随机排序、重复和删除等操作得到有效密文，不建议采用。其他更安全的加密模式，在增加安全性同时也会增加能耗，同时还要考虑加密模式的容错能力。表 3-15 列出了几种加密模式。CBC（Cipher Block Chaining）模式允许包丢失而不必重传。但研究表明，根据生日悖论，CBC 模式很容易造成信息泄漏。CFB（Cipher Feed Back）和 OFB（Output Feed Back）模式使用和分组一样大的反馈包，如表 3-9 所示。

表 3-9 模式比较

模 式	对密文的错误	对同步错误
CBC	一个错误位影响整个当前块和下一块相应位	受影响的区块需要重新转交下一块解密
CFB	一个错误位影响当前块相应位和下一块	受影响的区块需要重新转交下一块解密
OFB	一个错误位影响当前块相应位	受影响块并不需要重新转交
CTR	同 OFB	同 OFB

（1）RC5-32：在体积最优化和速度最优化的时候代码大小截然不同，在 OFB 模式下表现最突出。体积最优和速度最优的代码大小之比是 1∶1.5 。对于密钥初始化模式，在参考实现中用体积优化，在 OpenSSL 中用速度优化，两种实现的代码大小之比是 1∶1.2，运行速度之比是 1∶2，节省了代码存储但速度降低很多。

（2）RC6-32：RC6 的密钥初始化十分耗费时间，花费的 CPU 周期是加密阶段的 4 倍。体积最优化和速度最优化消耗的 CPU 周期没有大的差别。

（3）Rijndael：有 1 个大的 s 盒，所以代码存储超过 10KB。在 6 个加密算法中，是唯一解密要初始化密钥的，这个阶段耗费的时间是加密阶段初始化的 4 倍。虽然初始化密钥的代码大小是 RC6 的 2～3 倍，但运行速度是 RC6 的 50～70 倍。

（4）MISTY1：代码大小在 RC5、RC6 之间；在运行速度方面，也在 RC5、RC6 和 Rijndael 之间。它的速度优化模式实际上比体积优化模式要差（除了初始化密钥阶段 1）。

（5）KASUMI：初始化密钥是线性过程，但花费时间是 MISTY1 的两倍，代码大小比 MISTY1 大 40%～50%，加密运行速度比 MISTY1 好。和 MISTY1 一样，体积优化模式也比

速度优化模式运行速度快。

（6）Camellia：代码体积在所选算法中最大，速度优化比体积优化的代码体积大了50%，但运行速度几乎快了1倍。如表3-10所示，在初始化密钥阶段，MISTY1消耗最少的内存占有、CPU周期和最大的代码存储。Rijndael也在内存占用和速度方面有很好的排名，虽然RC5、RC6代码段比较小，但它们在内存占用和速度方面表现很差。

Camellia在代码存储上排名靠后，在运行速度上排名中间。KASUMI在各方面都表现平均。在加解密阶段，Rijndael运行速度最快，但同时要求很大的代码存储和内存占用，仅比Camellia稍好；MISTY1在各个方面表现都不错；KASUMI在各方面表现也很平均；RC5-32和Rijndael表现相反，速度降下去了，但代码大小和内存占用少；RC6-32的唯一优点是代码体积小；Camellia速度优化时运行速度比Rijndael慢，但代码体积约是RC5-32的10倍。总体而言，RC6-32可以说是能耗最多的加密算法，如表3-10所示。

表3-10 无线传感网加密算法的比较

项 目	顺序	存储优化			速度优化		
		代码量	数据量	速度	代码量	数据量	速度
密钥建立	1	RC5-32	MISIYI	MISIYI	RC6-32	MISIYI	MISIYI
	2	KASUMI	Rijndael	Rijndael	KASUMI	Rijndael	Rijndael
	3	RC6-32	KASUMI	KASUMI	RC5-32	KASUMI	KASUMI
	4	MISIYI	RC6-32	Camellia	MISIYI	RC6-32	Camellia
	5	Rijndael	RC5-32	RC5-32	Rijndael	Camellia	RC5-32
	6	Camellia	Camellia	RC6-32	Camellia	RC5-32	RC6-32
加密	1	RC5-32	RC5-32	Rijndael	RC6-32	RC5-32	Rijndael
	2	RC6-32	MISIYI	MISIYI	RC5-32	MISIYI	Camellia
	3	MISIYI	KASUMI	KASUMI	MISIYI	KASUMI	MISIYI
	4	KASUMI	RC6-32	Camellia	KASUMI	RC6-32	RC6-32
	5	Rijndael	Rijndael	RC6-32	Rijndael	Rijndael	KASUMI
	6	Camellia	Camellia	RC5-32	Camellia	Camellia	RC6-32

Camellia加密时需较高的能效，即使进行体积优化后，它的代码仍相当大；RC6-32和RC5-32密钥更新能力都较差，能耗较高；KASUMI相对MISTY1的优点是初始化密钥时的代码体积小。能耗最佳的算法，推荐使用Rijndael；硬件受限的情况下，推荐使用MISTY1。尽管MISTY1在初始化密钥时比Rijndael慢，但它比Rijndael消耗的存储量和CPU周期少；而且，加密时占用的内存小，代码大小只有Rijndael的一半。

MISTY1唯一的瑕疵是安全性比Rijndael低，且只提供单线加密，但有些应用情况对安全级别要求并不高。

OFB模式不但存储量小、能耗低，而且有良好的容错特性，即密文误差只影响当前组的相应比特的明文。因此，在容易出错的环境，如无线网络中，OFB尤为有用。但是，在密文丢失时的同步，CTR模式比OFB模式更容易重新同步，因为CTR是并行的。在能源效率上，CTR仅次于OFB，虽然CTR模式占有内存最大，但在同步纠正上有可能节省大量的内存，推荐使用CTR模式。

3.7.3 网络密匙和信任中心

由于传感器网络具有许多鲜明特点，因而对于安全方案的设计也提出了一系列挑战。一种比较完善的无线传感网解决方案应当具备如下基本特征：（1）机密性；（2）真实性；（3）完整性；（4）新鲜性；（5）扩展性；（6）可用性。

在传感器网络中，一个完整的会话密钥建立过程通常包括三个阶段，即密钥预分发、单跳密钥发现和多跳密钥建立。

（1）基站产生 n 个密钥及其对应的标识符（），这些密钥和标识符形成一个密钥池 P，即其中 k_i 为基站生成的密钥，ID_i 为密钥 k_i 对应的标识符。

（2）基站从 n 个密钥中随机选出 r 个密钥，组成某个传感器节点 A 的密钥环 RA，并将密钥环加载到 A 的存储器中，即其中 ID_{Ai}为密钥 k_{Ai}对应的标识符。基站保存每个传感器节点的密钥环（包括 r 个密钥及其对应的标识符）。

（3）传感器节点 A 计算与基站共享的密钥 K_{BA}并将其加载到存储器中。其中，ID_B 表示基站的身份标识。至此密钥预分发阶段结束，该阶段保证了簇内任意两个节点能够以某一概率在各自的密钥环上找到双方共享的会话密钥。

（4）传感器网络配置时，节点 A 被随机或者特定地散布在指定的感知区域内。在簇形成过程结束后，它广播一个信息，表示节点 A 所在簇内的任意节点，L_A 表示节点 A 的位置信息。

（5）收到该信息的所有节点将确信它在节点 A 的传输范围内，即两者在同一个簇中，并通过遍历其密钥环，检查是否存在与 A 广播的密钥标识符集相交的元素。假定节点 C 在其密钥环上发现存在与 A 标识符集相交的元素 ID_{AC}，则证明节点 C 与 A 共享有与 ID_{AC}对应的会话密钥 K_{AC}。

（6）A 使用共享会话密钥 K_{AC}对响应消息进行解密，确信其密钥环与节点 C 有交集。单跳密钥发现过程使得节点能够通过广播消息的方式，找到簇内与其共享有密钥环上某个会话密钥的节点。在单跳密钥发现过程结束后，节点 A 保存已找到共享实体的密钥，并将密钥环上其余密钥删除。

（7）对于簇内尚未与 A 建立共享密钥的节点来说，可以通过如下过程生成会话密钥。假定节点 D 在单跳密钥发现过程结束后，仍未与节点 A 建立共享密钥，但它找到与节点 C 共享的会话密钥 K_{DC}，且节点 A 与节点 C 也共享有密钥 K_{AC}。此时，A 发送一个挑战信息给节点 C 在对其进行身份认证后，该信息包含 A 和 D 共享的密钥 K_{AD}及 A 的位置信息 L_A。

（8）节点 C 解密消息，并将其使用密钥 K_{DC}对消息再次加密后转发给节点 D。$C \rightarrow D$: $\{K_{AD}, L_A\}K_{DC}$。

（9）节点 D 验证挑战消息的合法性，并发送一个响应信息给节点 A。$D \rightarrow A$: $\{Nonce, L_D\}K_{AD}$。其中，Nonce 是一个随机数，L_D 是节点 D 的位置信息。

（10）节点 A 使用共享密钥 K_{AD}对响应消息进行解密，确信与 D 共享的密钥已经建立。

在多跳密钥建立过程结束后，簇内任意两个节点之间都共享有一个会话密钥。传感器网络中的会话密钥建立后，任意两个节点之间即可遵循消息加密协议进行安全通信。

（1）假定节点 A 需要与节点 C 进行通信，首先计算加密密钥 Ke 和认证密钥 Km。

(2) 节点 A 使用加密密钥、认证密钥和计数器 C 对消息 M 进行加密并将其发送给节点 C。

(3) 节点 C 收到 A 发送来的消息后，重新根据共享密钥 KAG 来计算 Ke 和 Km，并验证消息的合法性。

节点 A 和 C 在会话过程中，使用了共享密钥 K_{AC} 对消息进行了加密，节点 C 和 D、D 和 A 在会话密钥建立时也采取了相应的共享密钥加密的方法，使得攻击者无法获知传输消息的内容，因而机密性得到了保证。由于通信双方共享唯一的会话密钥，该会话密钥具有与数字签名相似的身份认证功能，接收者可以通过数据源认证确信消息是从正确的节点处发送过来的，从而确保了消息的真实性。消息认证码要求将共享密钥和待检验的消息连接在一起进行散列运算，根据散列函数的强无碰撞特性，对数据的任何细微改动都会对消息认证码的值产生较大影响，从而能够有效地防止攻击者对截获的信息进行篡改，保证了消息的完整性。

共享密钥加密确保了攻击者无法获知和篡改计数器的信息，计数器的内容又能使接收者确信收到的数据是在最近时间内生成的最新数据，即消息是新鲜的。

会话过程不需要基站的参与，认证密钥和加密密钥可由通信双方根据共享的会话密钥自主地计算，从而有效地降低了基站的工作负荷，避免基站成为网络通信的瓶颈，这使得方案具有很好的可扩展性。由于引入了认证密钥、加密密钥和计数器，本方案具备了身份验证、消息保密和内容保鲜等诸多功能，并能够有效防止各种攻击（如重放攻击），从而使得其可用性大大提高。

在构建传感器网络加密方案时，充分考虑到节点计算速度、电源能量、通信能力和存储空间非常有限的特点，会话密钥建立协议和消息加密协议都设计得比较简单，参与各方在通信过程中需要传输的内容尽可能的少，并采取科学的分簇方法，合理确定簇的规模，确保通信的质量，减少因节点通信能力有限造成会话失败的几率。同时，本方案避开了代价昂贵的公钥运算，通过引入对称密钥、散列算法和计数器，来达到公钥基础设施的类似功能，并通过减少会话步骤、简化计算方法来降低节点的工作负荷，从而使得整个方案的计算、存储和通信开销都非常小，大大提高了方案的执行效率。

3.7.4 商业级加密无线传感网

ZigBee 应用程序使用 IEEE802.15.4 无线标准通信，本标准规定了两层物理层和 MAC 层。ZigBee 在这些层面上建立了 NWK 层和 APL 层。物理层提供了物理频段的基本通信能力。MAC 层保证了设备之间可靠的单跳通信连接。ZigBee NWK 层提供了创建不同网络拓扑结构所需的路由和多跳函数，例如星型、树状和网状结构。APL 层包括 APS 子层和 ZDO 和应用程序。ZDO 负责整体设备管理。APS 层提供了服务 ZDO 和 ZigBee 应用的基础。该架构包括在协议栈三个层次的安全机制。MAC 层、NWK 层和 APS 层负责安全运输各自的帧。此外，APS 子层提供建立和维护安全关系的服务。ZDO 管理设备的安全策略和安全配置。

ZigBee 安全服务包括密钥建立、密钥传输、帧的保护和设备管理。这些安全服务形成了 ZigBee 设备内实施安全策略的结构单元。

ZigBee 安全架构提供的安全级别取决于对称密钥的保管，采用的保护机制和密钥机制

与相关安全策略的合适执行。对安全架构的信任最终简化为对设定安全初值，安装密钥信息的信任和密钥信息的安全处理和储存的信任。在间接选址的案例中，假定信任绑定的管理程序。

安全协议的执行，例如密钥的建立，假定执行完整的协议，不遗漏任何步骤。随机数发生器假定如期运作。还有，假定设备外不安全方式不可能获得密钥，也就是说，除非密钥受到保护，例如在密钥传输中，一个设备不会有意地或者无意地传送密钥信息给其他设备。假定的一个例外情况发生在当一个没有预先配置的设备接入网络中。在此情况下，单个密钥会未受保护地发送，会引发对网络简短的攻击。

由于成本限制，ZigBee 假定不同的应用，可以使用逻辑不分开的相同无线设备，比如使用防火墙。再者，从特定设备的角度看，甚至不可能去证实另一个设备不同应用之间的密钥分离（除非认证），或者此协议栈的不同网络层之间有没有被合适地执行。因此必须假定使用相同频段的各自应用互相信任。这也就是说，没有密钥任务分离。另外，低一些的网络层（比如 APS 层、MAC 层或者 NWK 层）是任何应用都能完全可用的。这些假定形成设备的一个开放式信任模式。协议栈的不同网络层和单个设备的所有应用互相信任。

3.7.4.1　安全设计选择

设备上开放式信任模式有深远影响。它可以重复使用同一设备不同网络层上相同的密钥信息，它允许在设备到设备的基础上实现端到端的安全而不是两个通信设备中两个特定层之间（或者两个应用程序之间）。

另一个考虑是关注恶意网络设备通过网络允许可运输协议帧的能力。

这些意见中可以得出以下架构设计选择：

（1）首先，建立这样一个原则“最初产生帧的那一层负责对其进行加密”。例如，如果一个 MAC 层分离帧需要保护，MAC 层的安全服务应当被使用。同样的，如果 NWK 层命令帧需要保护，NWK 层安全应当被使用。

（2）如果需要保护安全服务不被盗窃（网络恶意设备），NWK 层安全会被为所有帧使用，除了那些通过路由器和一个新加入的设备使用（直到新加入的设备接受网络密钥）。因此，设备只有加入了网络和顺利地接受了网络密钥才能将它的消息在网络上多个跃点之间传达。

（3）由于有开放式信任模式，安全服务可以基于重复使用每个网络层密钥。例如，激活的网络密钥可以用于获得 APS 层广播帧、NWK 网络层帧或者 MAC 网络层指令。密钥的重复使用有助于减少存储成本。

（4）端对端安全被激活，仅使源设备可以存取共享密钥。这样可以使信任要求被限制到信息不安全的设备上。另外，可以确保设备间路由信息实现独立于信任因素（因此注意力分离了）。

（5）为了简化设备的互用性，一个特定网络里所有设备和一个设备里所有网络层的安全级别应该相同。尤其是 PIB 和 NIB 中显示出来的安全级别应该一样。如果一个应用因为该网络的净负荷超过额定载荷需要更多安全服务，该应用应该形成它自己更高安全级别的独立网络。

（6）有一些策略，任何真正执行的策略都必须正确选址。应用概况应包括的策略

如下：

1）处理由获得和未获得数据包引起的误差状况，有些误差状况可能显示安全资料的不同步或者不断攻击。

2）检测和处理计数器同步和计数器溢出损失。

3）检测和处理密钥同步损失。

4）如有需要，终止和周期性升级密钥。

3.7.4.2 安全密钥

ZigBee 设备间安全基于一个连接密钥和一个网络密钥。APL 同等实体之间单播通信是由 128B 两设备间的连接密钥获得的。广播通信是由 128B 网络上所有设备间共享的网络密钥实现的。指定的接受者一直了解准确的安全安排，也就是说，接受者知道网络帧是由连接密钥还是网络密钥来保护的。

一个设备可以通过密钥传输，密钥建立或者预安装（比如在工厂安装期间）来获得连接密钥。一个设备可以通过密钥传输，或者预安装来获得网络密钥。通过密钥建立技巧来获得连接密钥基于一个控制密钥。一个设备可以通过密钥传输或者预安装来获得控制密钥（为了建立相应的连接密钥）。最终，设备之间的安全取决于这些密钥的初始化设置。

在一个安全的网络中可以找到一系列的网络服务。注意，不同的安全服务要避免重复使用密钥，由于不需要的相互作用否则可能会导致安全漏洞。因此，这些不同的服务使用的一个关键来自单向函数使用链接密钥。使用无关密钥保证了不同安全协议执行的逻辑分离。密钥载入保护了传输的控制密钥，传输密钥保护了传输的其他密钥。

网络密钥归 ZigBee 的 MAC、NWK 和 APL 层使用。如此，每层应该有同样的网络密钥和相关的输出的和输入的帧计数器。连接密钥和控制密钥应该只在 APL 层找到。

3.7.4.3 信任中心作用

为了安全起见，ZigBee 定义了信任中心的作用。信任中心是设备网络内值得信赖的装置，为网络和端到端应用的配置管理分发密钥。该网络所有成员应承认一个信任中心，并且每一个安全的网络只能有一个信任中心存在。

在高安全级别商用的应用中，一个设备可以预先装载信任中心和初始控制密钥（例如通过未特别指出机制），如果应用可以忍受一小会攻击，控制密钥可以通过频带内未加密密钥传输。如果没有预先装载，设备的信任中心默认是 ZigBee 的协调器或协调器指定的设备。

在低安全级别中，家居应用，一个设备使用网络密钥和信任中心通信，可以通过预先安装或者通过频带内不加密密钥传输。

信任中心的功能可分为三个：信任管理器、网络管理器和配置管理器。装置信任管理器，以确定设备作为网络和配置管理器的功能。网络管理器负责维护网络的网络密钥。配置管理器负责绑定两个应用程序，使设备之间端对端管理安全（例如通过分配控制密钥或链接密钥）。为了简化信任管理，这三个作用载在一个单一的设备中——信任中心。

为了信任管理，一个设备应该接受通过未加密的密钥传输来自其信任中心的一个初始主密钥或者活动网络密钥。为了网络管理，一个设备只能从它的信任中心接受一个初始的

活动网络密钥和最新的网络密钥。为了配置，一个设备只能从其信任中心接受主密钥和连接密钥，用于建立两个设备之间端到端的安全。除了初始主密钥和网络密钥，额外的连接密钥、主密钥，以及网络密钥只能有它们来自一个设备的信任中心时，通过加密的密钥传输接受。

3.7.4.4 MAC 层安全

当 MAC 层产生的帧需要保护时，ZigBee 应该用 802.15.4 规定的 MAC 层安全服务。一个安全的勘误建议发展了 MAC 层规范，包含了 ZigBee 中的安全因素。

详细地说，至少其中一个安全因素是需要保护基于 CCM* 安全级别输入和输出的网络帧。CCM* 包含 CCM 的所有特征，并且附加仅编密码和仅集成能力。这些附加的能力消除了 CTR，CBC-MAC 模式的需要简化了安全程序。另外，与其他每个安全级别都需要一个不同密钥 MAC 层安全模式不同，CCM* 的使用使每个安全级别都使用一个安全密钥，CCM* 的使用使整个 ZigBee 协议栈中 MAC 层、NWK 层和 APS 层都可以重复使用一个密钥。

MAC 层负责它自身安全程序处理，上层应该决定使用哪个安全级别，对于 ZigBee 来说，MAC 层帧要求从 MACPIB 属性 macDefaultSecurityMaterial 或 macACLEntryDescriptorSet 中获取安全资料。上一层（比如 APL）应该设定 macDefaultSecurityMaterial 属性值和活动的 NWK 层网络密钥和计数器一致，也应该设定 macACLEntryDescriptorSet 属性和邻设备 APL 层的连接密钥，例如父与子。安全套装应该使用 CCM*，上一层应该设定安全级别和 NIB 中 nwkSecurityLevel 属性一致。对于 ZigBee 来说，应该使用 MAC 层连接密钥，将使用默认密钥（macDefaultSecurityMaterial）。图 3-108 展示了包含在 MAC 层输出帧安全域的一个案例。

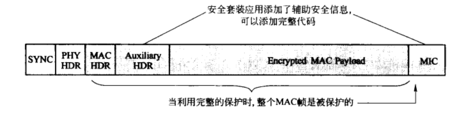


图 3-108　MAC 输出帧安全域

3.7.4.5 NWK 层安全

当 NWK 层产生的帧 nwkSecurityLevel > 0，或者上层的 NIB 中 nwkSecureAllFrames 属性为 TRUE. ZigBee 时应该使用帧保护机制。除非 SecurityEnable 参数 NLDEDATA. request 原语是 FALSE，明显显示了安全。像 MAC 层一样，NWK 层帧保护机制应该使用（AES），并且使用 CCM*。适用 NWK 层的安全级别在 NIB 中 nwkSecurityLevel 属性中给出。更上一层通过建立活动的和轮换的网络密钥来管理 NWK 层安全和决定使用哪个安全级别。

NWK 层的一个任务就是给信息在多跳连接中路由。作为本任务的一部分，NWK 层会广播路由要求信息并且处理接收到的路由回复信息。路由要求信息被同步广播到邻近的设

备并且传递邻近的设备回复的信息。如果可以利用合适的连接密钥，NWK 层会使用连接密钥去获得输出 NWK 帧，如果不能利用合适的连接密钥，为了不受外界干扰获得信息，NWK 层应该使用网络密钥去获得输出的 NWK 帧。

在本纲要中，帧格式明了地显示了保护帧的密钥，因此，设定的接受者可以推论出为处理输入帧该使用哪个密钥，也决定了信息在所有网络设备中可读而不是仅仅自己可读。图 3-109 展示了 NWK 层包含的安全域的一个案例。

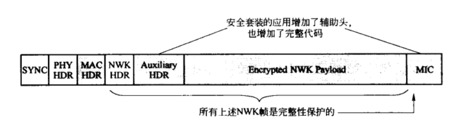


图 3-109 NWK 安全域

3.7.4.6 APL 层安全

当 APL 层产生的网络帧需要保护，APS 子层应该处理安全问题。APS 层负责安全传输输出帧、输入帧，建立和管理密钥所需步骤的安全，上层通过发出原语到 APS 层控制密钥管理。APS 层允许帧安全基于连接密钥或者网络密钥。图 3-110 展示了 APL 层包含的安全域的一个案例。APS 层的另外一个安全责任就是提供应用和带有密钥建立，密钥传输和设备管理服务的 ZDO。

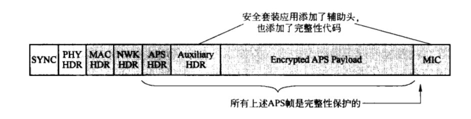


图 3-110 APL 安全域

APS 子层的密钥建立服务提供了 ZigBee 设备得到和其他 ZigBee 设备共享的连接密钥的机制。密钥建立涉及两个实体，一个发出设备和一个响应设备，必须先通过信任认证步骤。

信任信息（比如一个主密钥）提供了建立连接密钥的起点，可以在频带内或者频带外供配置，一旦配置了信任信息，一个密钥建立协议包括如下三个概念步骤：

（1）交换短暂数据。

（2）适应短暂数据去获得连接密钥。

（3）确认连接密钥被正确地计算。

在 SKKE 协议中，一个发出装置建立一个带有使用控制密钥的响应设备。这个控制密

钥，例如说，可能会在制造过程中预装，也可能在信任中心安装（例如，发出设备、响应设备或者第三方设备作为一个信任中心），或者基于一个用户输入的数据（例如 PIN 码），控制密钥的秘密性和权威性应该得到支持来获得信任基础。

密钥运输服务提供担保和无担保手段运送一密钥到另一设备或其他设备。担保密钥运输命令提供了一种手段来运输控制密钥、链接密钥或网络密钥由一个密钥源（例如，信任中心）到其他设备。无担保密钥运输命令提供了一种手段加载装置初始密钥。这个命令不加密保护正在加载的密钥。在这种情况下，密钥运输的安全可用非加密手段实现。例如，通过频带外频道传递保证秘密性和真实性。

更新设备的服务为设备提供了一种安全手段（例如，路由器）通知第二装置（例如，一个信任中心），第三个设备已经改变了地位，必须更新（例如，该器件加入或离开了网络）。这一机制的信任中心设有一个准确的名单，列出活跃的网络设备。

移除设备服务提供一个安全的手段，设备（例如，一个信任中心）可能会通知其他设备（例如路由器）的一个子设备应从网络去掉。例如，这可能被采用从网络移除没有满足信任中心网络设备安全要求的设备。

请求密钥服务提供了一种安全的从另一装置（例如，其信任中心）设备请求当前的网络密钥手段，或端到端应用控制密钥。

转换密钥服务提供一个安全的手段，设备（例如，一个信任中心）通知其他设备应该转换到不同的活动的网络密钥。

3.8 无线传感网高级技术——能量管理

无线传感网节点一般是静止不动的，并可能处在野外恶劣的环境中，不允许更换电池，因此无线传感网节点的能源管理问题是延长无线网络传感器应用寿命和降低成本的关键，成为无线传感网的研究的核心问题之一，涉及两个方面问题，即供能与耗能问题。

因此要解决无线传感网节点的能源管理问题也必须从这两个方面进行深入细致的研究。目前在解决耗能问题方面研究较多，例如为了有效利用现有能量资源，延长网络的生命周期，研究各种优化的路由通信协议等。像所有生物系统不可能只通过无限地降低自身消耗不补充能量而能够长久维持系统正常状态一样，无线传感网节点也不可能仅靠各种优化降耗的方法使得节点长期正常工作下去，当各种措施使得能耗已经降低到一定限度后，人们再努力也将得不到更好的效果。

因此我们必须从能量供应的角度进行研究，采取有效的方法为无线网络传感器提供源源不断的能量供应。如同任何生物系统都能够从周围环境中获取并储存能量那样，无线传感网节点也可以从其所处环境中获取并储存能量，所以研究如何从环境中有效地采集和储存能源能量的收集方法越来越受到研究者的重视。

3.8.1 微处理器和无线单片机节能技术

传感器节点通常是一个微型嵌入式系统，它的处理能力、存储能力和通信能力相对较弱，通过携带能量有限的电池供电。在不同应用中，传感器节点的组成不尽相同，但一般都由数据采集（传感器模块）、数据处理（微处理器模块）、数据传输（无线通信模块）和电源管理这 4 部分组成。因此微处理器的低功耗是无线传感网节能技术的关键之一。

随着集成电路技术和工艺的飞速发展，真正单片化的无线片上系统SOC（无线单片机）已经成为主流产品。它的绝大部分资源都在单片芯片内部，过去需要用外部扩展器件才能实现的功能，如ROM、RAM、A/D、D/A、数字量I/O、显示驱动等功能，现在在无线单片机内部就可以完成。

单片机的真正单片化，省去了大量的硬件开发调试工作，大大地提高了工作效率。系统先天的可靠性、抗干扰能力得到了显著的改善。经实验测试，实现同样功能的系统，采用单片方式比总线扩展方式具有更多的优点。系统不仅功能强、性能可靠、成本降低，而且进一步微型化和便携化。因此使用电池作为系统的电源也越来越普遍。

系统的最小电源消耗和最大的电池寿命就成为主要的技术要求。例如1999年的多国仪器仪表展览会上，不止一家国外公司展出了使用电池的工业流量计，5～10年都不必更换电池和进行维护。所以低功耗单片机的应用有着非常广阔的天地。

低功耗单片机应用符合现代电子终端产品的要求：便携、节能、可靠等。目前国际上先进的单片机生产厂商，如日本NEC、富士通、爱普森和美国TI等公司都采用了低功耗设计。在一些应用中使用了无线单片机CC2430，其休眠状态下的功耗电流可达到0.5～0.1μA。

无线单片机低功耗设计技术简要概括如下：

（1）高集成度的完全单片化设计。将很多外围硬件集成到了CPU芯片中，增大硬件冗余。内部以低功耗、低电压的原则设计，这给单片机的低功耗设计提供了很强的支持。

（2）内部电路可选择性工作。通过特殊功能寄存器选择使用不同的功能电路，即依靠软件选择其中不同的硬件。对于不使用的功能使其停止工作，以减少无效功耗。

（3）宽电源电压范围。先进的单片机芯片工艺特点决定了单片机在很宽的电源电压范围内都能正常工作。例如NEC公司78K0S系列的单片机，可以在1.8～5.5V电源电压范围内正常工作。单片机供电电压范围的放宽，可以进一步拓宽单片机的应用领域，尤其是便携式或掌上型仪器或装置可以放心地使用电池作为电源，而不必关心电池放电过程电压曲线是否平稳、是否会影响单片机正常工作，更不必因电池供电而专门增加稳压电路，从而可减少大约1/3的功率消耗。

（4）具有高速和低速两套时钟。系统运行频率越高，电源功耗就会相应增大。为更好地降低功耗，内部集成了两套独立的时钟系统，高速的主时钟和32.768kHz的副时钟。也可在满足功能需要的情况下按一定比例降低CPU主时钟频率，以降低电源功耗。在不需要高速运行的情况下，可选用副时钟低速运行，进一步降低功耗。通过软件对特殊功能寄存器赋值可改变CPU的时钟频率。或进行主时钟和副时钟切换。

（5）在线改变CPU的工作频率。可根据CPU处理任务的不同，在外部振荡器不变的情况下，通过程序改变处理器时钟控制寄存器PCC的值，在线改变CPU的频率。CPU在几种不同频率下工作的电源功耗差异非常大。

（6）后备功能。后备功能是为了进一步降低系统功耗。CPU用主时钟时有HALT（待机）模式和STOP（休眠）模式，用副系统时有副时钟运行模式和HALT模式。

（7）内部钟表定时器。无线单片机内部提供了时钟定时器，每隔几个毫秒产生一次中断。在系统处于休眠状态时，仍可定时被唤醒。对于无线单片机只需间歇工作但又需要实时计时功能的应用场合，提供了非常有效的节能方法。微处理器在不工作时可进入STOP

模式或 HALT 模式，进入低功耗的后备功能状态。当时钟中断到来时，微处理器回到正常工作状态，进入时钟中断处理程序做时钟更新处理，然后再进入后备功能状态。

（8）低功耗模式。低功耗模式指的是系统的等待和停止模式。处于这类模式下的单片机功耗将大大小于运行模式下的功耗。过去传统的单片机，在运行模式下有 wait 和 stop 两条指令，可以使单片机进入等待或停止状态，以达到省电的目的。等待模式下，CPU 停止工作，但系统时钟并不停止，单片机的外围 I/O 模块也不停止工作；系统功耗一般降低有限，相当于工作模式的 50% ~70%。停止模式下，系统时钟也将停止，由外部事件中断重新启动时钟系统时钟，进而唤醒 CPU 继续工作，CPU 消耗电流可降到 μA 级。在停止模式下，CPU 本身实际上已经不消耗什么电流，要想进一步减小系统功耗，就要尽量将单片机的各个 I/O 模块关掉。随着 I/O 模块的逐个关闭，系统的功耗越来越小，进入停止模式的深度也越来越深。进入深度停止模式无异于关机，这时的单片机耗电可以小于 20nA。

其中特别要提示的是，片内 RAM 停止供电后，RAM 中存储的数据会丢失，也就是说，唤醒 CPU 后要重新对系统作初始化。因此在让系统进入深度停止状态前，要将重要系统参数保存在非易失性存储器中，如 EEPROM 中。深度停止模式关掉了所有的 I/O，可能的唤醒方式也很有限，一般只能是复位或 IRQ 中断等。

保留的 I/O 模块越多，系统允许的唤醒中断源也就越多。单片机的功耗将根据保留唤醒方式的不同，降至 1μA 至几十 μA 之间。例如，用户可以保留外部键盘中断，保留异步串行口（SCI）接收数据中断等来唤醒 CPU。保留的唤醒方式越多，系统耗电也就会多一些。其他可能的唤醒方式还有实时钟唤醒、看门狗唤醒等。停机状态较浅的情况下，外部晶振电路还是工作的。

单片机应用系统中的低功耗设计要注意的问题如下：

1）系统中单片机以外的其他电路器件尽可能选用静态功耗低的器件，如选用 CMOS 电路芯片。

2）外部设备的选择也要尽可能支持低功耗设计。

3）设计外部中断唤醒电路，使单片机在等待时可进入休眠模式或待机模式，需要时由外部中断信号唤醒。

4）设计外部器件的电源控制电路，使外部器件或设备在不工作时关断供电，减少无效功耗。

5）设计充分利用系统低功耗特点的软件。

（9）用“中断”代替“查询”。一个程序使用中断方式还是查询方式对于一些简单的应用并不那么重要，但在其低功耗特性上却相去甚远。使用中断方式，CPU 可以什么都不做，甚至可以进入等待模式或停止模式；而查询方式下，CPU 必须不停地访问 I/O 寄存器，这会带来很多额外的功耗。

（10）用“宏”代替“子程序”。程序员必须清楚，读 RAM 会比读 Flash 带来更大的功耗。正是因为如此，低功耗性能突出的 ARM 在 CPU 设计上仅允许一次子程序调用。因为 CPU 进入子程序时，会首先将当前 CPU 寄存器推入堆栈（RAM），在离开时又将 CPU 寄存器弹出堆栈，这样至少带来两次对 RAM 的操作。因此，程序员可以考虑用宏定义来代替子程序调用。对于程序员，调用一个子程序还是一个宏在程序写法上并没有什么不同，但宏会在编译时展开，CPU 只是顺序执行指令，避免了调用子程序。唯一的问题似乎

是代码量的增加。目前，单片机的片内 Flash 越来越大，对于一些不在乎程序代码量大一些的应用，这种做法无疑会降低系统的功耗。

（11）尽量减少 CPU 的运算量。减少 CPU 运算的工作可以从很多方面入手：将一些运算的结果预先算好，放在 Flash 中，用查表的方法替代实时的计算，减少 CPU 的运算工作量，可以有效地降低 CPU 的功耗（很多单片机都有快速有效的查表指令和寻址方式，用以优化查表算法）；不可避免的实时计算，算到精度够了就结束，避免“过度”的计算；尽量使用短的数据类型，例如，尽量使用字符型的 8 位数据替代 16 位的整型数据，尽量使用分数运算而避免浮点数运算等。

（12）让 I/O 模块间歇运行。不用的 I/O 模块或间歇使用的 I/O 模块要及时关掉，以节省电能。RS232 驱动需要相当的功率，可以用单片机的一个 I/O 引脚来控制，在不需要通信时，将驱动关掉。不用的 I/O 引脚要设置成输出或设置成输入，用上拉电阻拉高。因为如果引脚没有初始化，可能会增大单片机的漏电流。特别要注意有些简单封装的单片机没有把个别 I/O 引脚引出来，对这些看不见的 I/O 引脚也不应忘记初始化。

低功耗无线单片机的应用使电子产品、控制系统、无线传感网更符合当今时代的要求，达到便携、低功耗和高可靠性。加之用高级语言（如 C 语言）对无线单片机进行开发的工具日臻完善，更为快速高效的开发应用提供了良好的条件和环境。低功耗的节能无线单片机应用系统将会带来很好的社会效益和经济效益。

3.8.2 低功耗节点设计技术

自组织传感器网络最大的特点就是能量受限。传感器节点受环境的限制，通常由电量有限且不可更换的电池供电，所以在考虑传感器网络体系结构以及各层协议设计时，节能是设计的主要考虑目标之一。

传感器节点消耗能量的模块包括传感器模块、处理器模块、无线通信模块，其中处理器和传感器模块的功耗很低，绝大部分能量消耗在无线通信模块上。传感器节点传输信息比执行计算时更消耗电能，传输 1B 信息 100m 距离需要的能量相当于执行 3000 条计算指令消耗的能量。要降低网络化传感器的硬件部分的功耗，首先要合理地选择传感器系统的技术指标。在一个系统中，往往有很多技术指标都是和功耗联系在一起的，如速度、驱动能力、稳定性、线性度等，这些技术指标的提高往往都是以提高电路的功耗来换取的。因此应该根据传感器的特点和需要，合理地选择系统的技术指标，在某些情况下，甚至降低某些非关键性指标，以达到降低系统功耗的目的。在技术指标确定的情况下，从硬件方面考虑降低网络化传感器的功耗包括两个方面，即降低信号获取单元消耗的功率以及降低信号处理单元消耗的功率。

本节所设计的节点配备了基本的无线收发模块、微控制器模块、电源模块和 I/O 扩展接口。该节点的硬件设计综合考虑了功耗和性能等诸多方面，较之现在主流节点（如 telosB、micaz 等），本章设计的节点采用了功耗更低的处理器芯片和性能更好的射频收发器芯片。

处理器和无线收发模块是节点的两个关键模块，本节所设计的节点选择了超低功耗处理器 MSP430F2618 和工作在 ISM 自由频段的 ZigBee 射频芯片 CC2520。处理器模块是数据处理、进程调度的核心单元，一般由 MCU 和扩展的存储器组成。根据 WSN 的低功耗要

求，MCU 芯片的选择标准包括：工作模式、工作电流、工作电压、唤醒时间等。无线通信模块是 WSN 组网以及 WSN 与信息世界相连接的重要模块，一般由无线收发芯片和相应频率的天线组成。由于 WSN 的无线通信倾向于无线电通信，所以选用工作在 ISM 自由频段的射频芯片。节点电路示意图如图 3-111 所示。

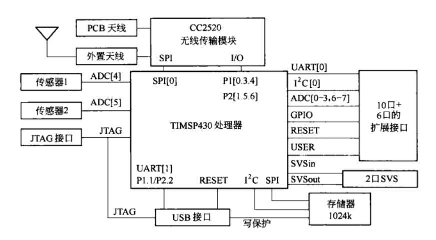


图 3-111 电路示意图

微处理器和 CC2520 之间通过 SPI、GPIO、VREG-EN 和 RESETn 信号进行连接。SPI 提供一个接口，通过该接口实现微处理器和 CC2520 之间的数据传递。CC2520 有 6 个 GPIO 可以根据需要和微处理器进行连接。CC2520 的工作模式有激活模式和两种低功耗运行模式。微处理器通过 VREG-EN 信号控制 CC2520 工作于低功耗模式。微处理器通过 RESETn 信号使 CC2520 在上电时复位。微处理器和 3 个不同颜色的 LED 连接，通过灯的闪烁和颜色变化显示节点的工作状态。微处理器通过 SPI 接口和控制信号外接 EEPROM，用来存储日志数据或相关数据。

低功耗设计中，传感器节点使用的处理器应该满足功耗低且支持睡眠模式，处理器功耗主要由工作电压、运行时钟、内部逻辑复杂度以及制作工艺决定，工作电压越高，运行时钟越快，其功耗也越大。目前，使用 5 号电池供给单片机的无线传感器节点，满负荷工作只能持续十几个小时，为了让这样的系统工作一年的时间，系统需要在绝大多数时间内处在待机或者睡眠状态。这就要求处理器必须支持超低功耗的睡眠状态。本系统中采用 TI 公司的 MSP430F2618。

MSP430 系列微控制器为 16 位 RISC 架构，集成大量的寄存器和数据存储器，本节采用 MSP430，其 RAM 也可以参与运算。在运算速度方面，MSP430 微控制器能在 8MHz 晶体的驱动下，实现 125s 的指令周期。16 位的数据宽度、125s 的指令周期以及多功能的硬件乘法器（能实现乘加）相配合，甚至能实现数字信号处理的某些算法。

MSP430 芯片能够工作在 1.8 ~ 3.6V 电压范围内，在只有 RAM 数据保持的低功耗模式下，消耗电流仅为 0.1A。它具有 5 种节电工作模式，在不同的模式下消耗电流在 0.1 ~ 400A 之间，待机模式下消耗电流仅为 0.8A。一般情况下，可将 CPU 置于省电模式。

由于无线通信占了整个 WSNs 能耗的主要部分，因此对无线收发系统的能耗管理非常重要，采取以下措施可以减少通信模块的能量损耗：

（1）增加休眠时间。无线通信模块存在发送、接收、空闲和睡眠4种状态，无线通信模块在空闲状态一直监听无线信道的使用情况，检查是否有数据发送给自己，而在睡眠状态则关闭通信模块。无线通信模块在发送状态的能量消耗最大，而在空闲状态和接收状态的能量消耗接近，略少于发送状态的能量消耗，在睡眠状态的能量消耗最少。要让网络通信更有效率，减少不必要的转发和接收，不需要通信时，尽快进入睡眠状态是传感器网络协议设计需要重点考虑的问题。

（2）使用多跳短距离无线通信方式。无线通信消耗能量与通信距离 d 的关系为 $E = kd^n$，式中，k 是一个常数，参数 n 满足关系 $2 < n < 4$，n 的取值与很多因素有关；例如传感器节点部署贴近地面时，障碍物干扰源多，n 的取值就越大，无线信道质量对信号发射质量的影响也很大，考虑诸多因素，通常取 n 为3，即通信能耗与距离的3次方成正比。随着通信距离的增加，能耗将急剧增加。因此，在满足通信速率的前提下，应该尽量减少单跳通信距离。一般而言，传感器节点的通信半径在 10011 以内比较合适。

采用的无线传输模块是具有 IEEE802.15.4/ZigBee 标准的 CC2520。此模块在不进行数据传输的时候，能够自动进入休眠模式，达到省电的目的。由于传输的数据对时延、传输速率要求不高，采用此种无线模块以求高性能价格比。

在系统的软件设计时，主要采取以下的具体措施来降低功耗：

（1）尽可能地采用待机和掉电运行方式以缩短 CPU 的运行时间，因为在单片机应用系统中，系统的功耗与 CPU 的工作时间长短成正比。

（2）外围功耗管理。停止 MCU 外围部件的无效操作。系统应对时钟和信号流进行控制与调度，禁止它们进入进行无效操作的外围电路，使得这些电路中的 CMOS 门处于静止状态，仅消耗静态功耗。

（3）外围电源管理。对系统中的一些非 CMOS 功耗特性电路或一些模拟电路不能采用关断时钟和信号流的方式来达到最小功耗，而是必须依靠电源供电管理方式。

（4）不要采用动态扫描显示方式，而利用锁存器采用静态显示方式，以减少 CPU 的工作时间。

（5）尽量少采用软件循环延时的工作方式，而采用中断的工作方式，可以减少 CPU 工作时间。

3.8.3 能量收集技术

无线传感网一般由数量庞大的传感器节点组成，并散布于一定区域内，通常采用电池提供能量。但是，由于受到节点体积的限制，所配置的电池能够提供的能量是非常有限的。同时，由于传感器节点经常处在恶劣环境或人员不能到达的环境中，另外传感器节点数量也非常大，因此无法为每个节点更换电池。所以，一个设计全面周到能够长久使用的传感器节点，必须从截流和挖潜两方面采取有效措施，以改善节点的能源供应。

所谓截流，就是要采取各种节能机制尽量减少节点的能量消耗，延长节点和网络的寿命。所谓挖潜，就是要采取各种方法为传感器节点补充能量。从一定意义上讲，挖潜比截流更能从根本上解决问题。挖潜的方法就是要从传感器节点所在的环境中获取一切可以利

用的能源，即所谓的能量收集。

无线传感网节点能量收集与使用中能量收集与储存单元从节点所处的环境中收集各种可资利用的能源并储存起来。当节点需要能源时，将能量从储存单元中取出经过变换得到节点上所需使用的总电源 VCC，通过 VCC 供电，节点上的各个元器件获得电源，例如模数转换器、微控制器、射频收发器等，保证传感器的电源需求，实现长期有效的供电。

根据传感器节点所处环境不同，环境中可以收集的能源也不相同，所以单一能源的能量收集方法难以保证无线传感网中所有节点均能可靠地获取到所需的能源。为此，有必要为每个传感器节点设置两种甚至更多种能源的能量收集方法，这就要求在有限空间的无线传感网节点内部，根据节点工作环境中可能的能源种类，尽可能配置综合的能量收集电源。

在我们生活的物质空间里可能存在着各种潜在的可以利用的能源，例如太阳（光）能、风能、热能、机械振动能、声能、电磁场能等。如何在小小的传感器网络节点上收集储存这些能源，是近年来许多科学家努力研究的焦点问题之一，目前也取得了一定的进展。其中，利用机械振动和光能的能量收集技术研究比较多，并有相关器件的产品出现，具有较好的应用前景。

3.8.3.1 振动能量的收集

各种各样的因素都会导致环境中产生振动，因此环境振动是普遍存在的，例如，用手在桌子上轻拍，桌子就产生振动，振动加速度可能达到 0.02g。利用压电材料的压电效应可以收集振动的能量。压电材料在受到力的作用时发生变形并产生极化电荷，将电荷转换成电压后就可以通过收集电路储存起来。

通过一个直径 4.6cm、高 4.6cm 的振动能量收集器收集 28Hz 100mg 的环境振动，可以获得 9.3mW 的电量。研究表明，收集器的体积增加一倍则收集到的电量也增加一倍；收集到的电量还与振动频率呈线性关系，与振动力成指数关系。因此国外许多研究者致力于压电能量收集器的研究，并取得了相当的进展，有关试验性产品已经推出。

3.8.3.2 太阳（光）能的收集

光电材料的新进展，使光能收集成为无线网络传感器能量来源的另一种耗之不竭的新方法，光电元件的安装和运行费用随着大规模的应用也可大大减少。

光电采集的基本原理是利用光电材料吸收大量的光子，如果光子足够多从而能激活光电池中的电子，经过适当的结构设计，电子可被获取。光电元件相当于解码器，在光的照射下产生电压，结合相应的调整和储存电路可为负载实现供电。电量的多少是收集的光能的函数，为获取较多的电量，光电元件通常置于光照好的环境，并增大光照面积。通常的光电池可产生电压 DC0.5V，但实际电压输出随运行温度的不同而变化，一般说来温度越低输出电压越高，光照越强电流输出越大。为了产生系统需要的电压，需要将多个光电元件进行串行连接。

光电技术发展从最初的硅晶体制造到今天微粒子沉积在感光基片上，这种新材料可在室内或室外工作，重量轻，易安装，并受环境温度的影响减小，非常适于为小型、远程的传感器提供电源。

3.8.3.3 风能的收集

环境中的风是无处不在的。利用随处可得而又未经开发的风能也是研究者致力研究的课题，必须要解决技术难度和制造成本这两个难题。Arling-ton 得州大学使用成熟的压电和机械技术很好地解决了这两个难题。采用压电器件制造出的这种小型发电机，可由 8 ~ 16km/h 的风力驱动，能为无线传感网节点提供 50mW 的功率。发电机的桨叶连到凸轮上，使围绕轴排成圆形的一串双压电晶片产生振荡。一个采用 APC855 陶瓷制造的双压电晶片可输出 0.935mW 的功率，由 11 个压电晶片组成的单元可输出 10.2mW 的功率。

3.8.3.4 热电能的收集

温差电技术研究始于 20 世纪 40 年代，于 20 世纪 60 年代达到高峰，并成功地在航天器上实现了长时发电。温差发电机具有体积小、重量轻、无振动、无噪音、性能可靠、维修少、可在极端恶劣环境下长时间工作的特点，适合用作小于 5W 的小功率电源，用于各种无人监视的传感器、微小短程通讯装置以及医学和生理学研究仪器。目前，相关产品已进入实用阶段。近几年来，温差发电机在民用方面也表现出了良好的应用前景。

1942 年，苏联研制成功最早的温差发电机，发电效率只有 1.5% ~2%，目前开发的温差发电机，效率也普遍处于 6% ~11%。通过对热电转换材料的深入研究和新材料的开发，不断提高热电性能，争取在热源不变的情况下提高电输出功率已成为温差电技术研究的核心内容。

德国科学家最近发明了一种利用人体温差产生电能的新型电池，可以给便携式微型电子仪器提供长久的“动力”，免去了充电或更换电池的麻烦。只要在人体皮肤与衣服等之间有 5℃的温差，就可以利用这种电池为一块普通的腕表提供足够的能量。

3.8.3.5 声能的收集

人造铌酸锂具有在高频高温下将声能转变为电能的特殊功能。当声波遇到屏障时，声能会转化为电能。英国科技人员根据这一原理，设计制造了鼓膜式接收器，将接收器与能聚集声能的共鸣器连接，当它把所收集的噪声输入声能变换器后，便可发出电来。据测定，当喷气式飞机的噪声达到 160dB 时，其发电功率可达 100kW。

新型热声学发动机由一个长棒球棍状的共振器与一个椭圆形的容器组成，没有把柄。发动机内盛有经过压缩的氦，当氦被加热时，就会产生声波，形成声能，这种声能可以启动活塞，产生电力。常规的发动机受热力学及发动机复杂性的限制，典型的、最有效的发动机是用于发电站的、巨大的涡轮机。小型声能发动机比最大型的、最有效的涡轮机的效力还要大 10%，而且没有运转部件，不必维护。

3.8.3.6 磁能的收集

地球上无处不存在磁场，有磁就有能量。因此，磁能是一种取之不尽、用之不竭的新能源。利用磁能开发的新型发动机由发电机和电动机组合而成，能有效运用电磁能量和纯永磁体能量来驱动做功的机器。这种发动机工作时无须外界补充能源，有独立的自循环再生系统，是永恒的不要花钱的纯绿色动力能源。

3.8.3.7 各种能源的能量综合收集

我们生活的环境中存在大量的形式各样的能源。不同的环境中能量存在的形式也不尽相同。为了使每个传感器节点都尽可能从所处的环境中获得所需的能量，必须设计这样一种能量收集系统，它不能只从某一种能源中收集能量，否则一旦所处环境中该种能源缺乏，那么该节点将不能长期可靠地工作下去。因此，有必要将多种能量收集方法集成在每个节点上。当然，其困难是不难想象的，主要表现在以下几个方面：（1）各种能量回收技术与方法目前还不成熟，还需要研究者进行大量的创新性研究；（2）各种能量收集组件必须满足传感器网络节点对尺寸的苛刻要求；（3）要确保各种能量收集组件能够协调一致地工作并将收集到的能量有效地储存起来。

无线传感网正成为多种应用领域极富吸引力的解决方案，但是节点能源问题一直困扰着设计者和使用者。本节对无线传感网节点的能量供应及其管理技术的现状进行了分析讨论。通过对无线传感网节点的能量收集原理、技术与方法的分析研究，指出节点能量问题应该从节能与供能两方面去解决，并对环境中存在的各种能源的收集原理与方法进行了分析，包括太阳能、风能、声能、振动、热电以及电磁场能等。为了使传感器节点能够长期、稳定、可靠地工作，必须采用多种方法从环境中吸取能量，为传感器节点源源不断地供应能量，从根本中解决传感器网络节点的能量供应问题。

3.8.4 能量收集传感器节点设计

能量挖掘装置，可以挖掘各类能量。各种环境能源丰富程度不同，太阳能晴空直射条件下为 100mW/cm^2，此外还有温差、振动等形式的能量。目前已经有利用环境能量为无线传感网节点提供能量的系统的研究和开发。譬如创业公司 Perpetuum 推出的 PMG7 微发电机，能从一个 100mg 振动中产生高达 5mW/3.3V 的输出功率。但是利用振动能量使得节点只能布置在能经常产生振动的区域，使节点的布撒环境受到限制，另外在间歇性的振动的条件下，系统也无法连续工作。

下面提出了一种基于太阳能的能量供给系统，该系统利用多级能量内存，结合能量管理与能量转移技术，使由太阳能电池采集到的能量得到合理的利用，从而构成具有自我管理能力的能量供给系统，实现了为无线节点永久性供电与无线传感网络无限使用的目的。

为了更好地解决传感器节点的能量供给问题，我们提出了基于太阳能的能量供给系统，由以下部分构成：能量挖掘装置，由太阳能电池板构成，负责将太阳能转化为电能。能量内存，包括主级能量内存和次级能量内存，由超级电容构成，负责存储太阳能电池采集到的能量，并为无线网络传感器节点供电。后备能量内存，由锂电池组成，是紧急情况下系统的能量来源。电源管理和控制部分，负责监控主级和次级能量内存和后备能量内存的能量大小状态，根据状态控制这些能量内存为系统供电，并且控制太阳能电池为能量内存补充能量。系统总体结构图如图3-112所示。

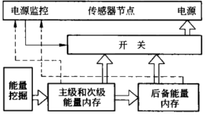


图 3-112 系统结构图

系统的主要操作模式是主级和次级能量内存

存储收集到的环境能量并且给传感器节点供电，而后备能量内存作为一个紧急情况下可靠的后备电源，使系统能够在环境能量间歇的条件下很好地工作。

能量挖掘装置采用的太阳能电池，效率大约是16% ~17%，在太阳直射情况下的输出功率约16 ~ 17mW/cm²。如果通过选择满足系统电压要求的配置来确定电压，可以将环境能源作为一个电源模型：

$$P_e(t) = P_{unit}(t) \times A(l)$$

式中，$P_{unit}(t)$是单位面积单位电池板的能量；A是并联起来的电池板的数目或是面积。

虽然能量内存的容量是有限的，但是为了尽可能多地从环境中摄取能量，那么$P_e(t)$应该尽可能高。这样，在给能量内存补充足够的能量之后，可以让系统继续利用环境能量。但是，太阳能板的大小应该结合系统性能指针、体积大小以及成本等因素综合考虑。

主级能量内存和次级能量内存由超级电容构成。作为节点最主要的能量来源，需要存储能量挖掘装置挖掘的能量，所以它应该能够经受频繁的充放电，而电容恰恰可以满足这个性能要求，而且大容量的超级电容能够提供足够的容量，因此，选用电容作为主级和次级能量内存是最为理想的。

为了延长主能量内存的供电时间，应根据漏电流、能量消耗水平以及系统启动时间的要求，确定合适的电容容量。根据报道，22F的电容漏电流最小。结合系统成本、体积方面的要求，选择25F的超级电容作为能量存储元件，通过将两个超级电容串联以减小其漏电流。

后备能量内存由锂电池构成。锂电池的特点有：漏电流低、能量密度高、单节电池电压高，因此，选择锂电池构成后备能量内存。然而必须注意，它需要复杂的充电电路以防止对电池的有害效应。

传感器节点在活动模式下和休眠模式下的功耗差别很大，功耗决定于三个参数：活动时间占总时间的百分比D，活动模式下消耗的电流I_a，以及休眠模式下的电流I_s。在大多数情况下，我们只对平均功耗P有兴趣（假设唤醒时间可以忽略）：

$$P = V_{sup} \times (D \times I_a + (l - D) \times I_s) \tag{3-2}$$

式（3-2）表示，I_a、I_s、V_{sup}和D都是影响系统功耗的因素，需要在实现时予以考虑。

在传感器节点上实现能量供应系统，该系统与一种节点通过一个40针的接口连接。系统采用一个60mm×60mm的太阳能电池板作为能量挖掘装置，它具有4.4V的输出电压。采用四个容量为25F的超级电容组成两级能量内存，每个有最大2.7V的额定电压。将两个超级电容串联起来作为一级能量内存，可以减小漏电流，并且与太阳能电池的输出4.4V匹配。采用容量为1120mA·h、工作电压为3.7V的锂电池作为后备能源。

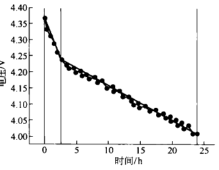


图3-113 漏电流曲线图

由两个25F电容串联构成的能量存储装置在漏电流的影响下测定的电压曲线如图3-113所示。测定时间范围为24h，为了反映能量存储装置的

总体趋势，采用分段线性的拟合方法，可以得出漏电流的变化规律如下：

$$V = \begin{cases} V_0 - 0.06t & 0 \leqslant t \leqslant 2.5 \\ V_0 - 0.15 - 0.0107(t - 2.5) & 2.5 \leqslant t \leqslant 24 \end{cases} \tag{3-3}$$

式中，V_0 为初始电压，单位为 V；t 为时间，单位为 h。

由以上可知，在 24h 内，超级漏电流的影响必须予以考虑，由于漏电流而损失的能量无法被系统利用。

由太阳能为超级电容组成的能量存储装置充电，太阳能电池的充电能量与超级电容的容电能量必须匹配，即在通常光照条件下，太阳能电池能为两级能量存储装置充满电量。

图 3-114 所示为能量存储装置的充电时的电压曲线。根据测量的电压值进行拟合，可以得到能量存储装置的充电电压曲线。拟合所得方程如下：

$$V = A(1 - e^{-Bx})^C \tag{3-4}$$

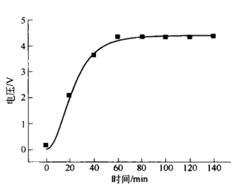


图 3-114 充电曲线

式中，A 为中止充电时的电压，即太阳能电池提供的电压，为 4.4；B、C 两个系数表征了充电时的外部条件如光照等，随外部条件不同，B、C 会有变化。在这条曲线中，B 为 0.06348，C 为 2.17868，拟合度为 99.766%，选择和能量内存匹配的太阳能电池必须以上述结果作为限制。

系统的控制部分使用 MSP430，用片上 AD 监控超级电容的电压确定其能量状态，实现对锂电池的保护以及对系统功耗和锂电池能量状态进行监测。测得节点活动模式下功耗为 48mA，查阅手册，低功耗模式下功耗为 35μA，根据式（3-2），如果节点活动周期为 1%，则平均功耗为(48mA + 99 × 35μA) ÷ 100，即为 515μA。

根据各级能量内存的能量大小状态，利用微处理器控制能量内存选择开关以控制太阳能电池为能量内存充电以及能量内存为系统供电，控制流程如下：

（1）启动系统（电池供电）。

（2）为主级能量内存充电。

（3）判断主级能量内存是否充满。若充满，则执行步骤 d。未充满，则执行步骤 b。

（4）由主级能量内存为系统供电，并为次级能量内存充电。

（5）判断次级能量内存是否充满：若充满，则执行步骤 f。未充满，则执行步骤 d。

（6）为主级能量内存充电，判断电池是否需要补充能量。若需要，则执行步骤 g。不需要，则执行步骤 h。

（7）为电池补充满能量。

（8）系统按上述步骤正常运转。

仿真节点工作在 1% 的工作周期下，则节点处于低功耗模式的时间为 99%，处于正常模式的时间为 1%，进行供电实验。在超级电容处于满电量的情况下，测定供电时间，根据多次实验，单级能量存储装置中的能量可供系统工作 745min。联机调试，以 1% 的工作

周期工作，系统平稳工作两天，初步证明系统可行。

3.9 无线传感网监控和分析

无线传感网中，各个分布的节点通过监测周围环境不断产生大量的感知数据。而无线传感器节点一般比较简单，存在存储能力低、能量受限等特点，无法像传统分布式数据库那样管理数据。如何存储、传输和访问这些数据，是无线传感网络应用的关键。

对于用户来说，无线传感网的核心是感知数据，而不是网络硬件。用户感兴趣的是传感器产生的数据，而不是传感器本身。用户经常会提出如下的查询："网络覆盖区域中哪些地区出现毒气"，"某个区域的温度是多少"，而不是"如何建立从 *A* 节点到 *B* 节点的连接"，"第 27 号传感器的温度是多少"。

综上所述，无线传感网是一种以数据为中心的网络，不同于以传输数据为目的的通信网络。对数据的管理和操作，成为无线传感网的核心技术。

从无线传感网体系（见图 3-115）中可看到无线传感网中传感器节点采集数据通过无线网络传输到数据中心进行数据管理，主要包括对感知数据的获取、存储、查询、挖掘和操作，目的就是把无线传感网上数据逻辑视图和网络物理实现分离开来，使用户和应用程序只需关心查询逻辑结构，而无需关心传感器网络实现细节。

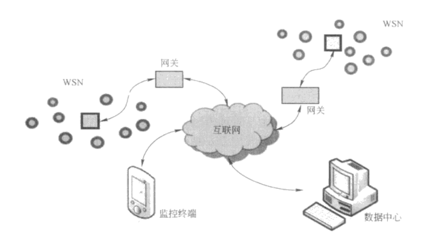


图 3-115 无线传感器网络体系

3.9.1 无线传感网远程遥控和监控

无线传感网由一定数目的传感器节点组成，以无线自组方式构成网络。无线传感网的监控是分层实现的，节点是监控平台最底层，向上依次为网关、数据中心、监控终端。传感器节点可安排在不相邻的区域内，从而形成多个传感器网络。传感器节点将采集到的数据传送到网关节点，网关节点负责将传感器节点传来的数据经由传输网络发送到数据中心。传输网络负责协调各网络的网关节点。数据中心对感知数据处理后传送到监控终端，并在本地的数据库中保存最新的节点感知数据。

监控终端按照应用需求对数据进一步分析与处理，得到所需要的数据，并进行图形化显示和性能分析，从而实现网络的监控，如图 3-116 所示。

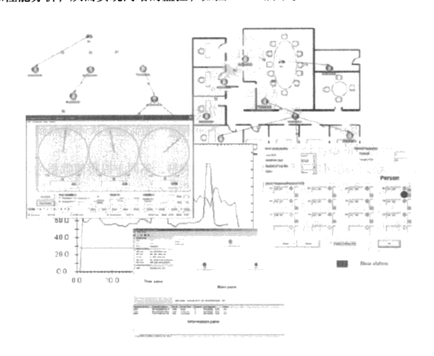


图 3-116 图形化监控

无线传感网监控平台的建立是为了管理传感器节点采集的各种环境数据并监控节点及整个网络的运行状态，并将这些数据转化为方便人们观察和查询的可视化信息，以便于实验开发和调试管理。因此该监控平台需要实现以下功能：

（1）对无线传感网原始数据收集。可以将传感器节点采集到的各种感知数据通过网关送到数据中心，并对原始数据进行储存，优化和处理。

（2）远程访问和控制。用户可以通过监控终端查阅数据中心数据而达到远程监控无线传感网的实时状态目的。

（3）友好的人机交互界面。通过人机交互界面，监控程序可以实现显示传感器节点的感知信息、节点能耗、路由状态，整个网络的拓扑结构状态以及移动节点的定位跟踪等功能。

（4）数据存储和管理功能。可以将大量的感知数据处理后按类存放到各自的数据库中，并能够实现离线状态的数据回放和查询。

（5）较好的可扩展性。在不同的应用背景下，需要处理不同的感知数据，能够根据应用的需要对传感器网络监控平台进行模块化扩展。

（6）较好的通用性。在数据包中增加传感器节点类型字段，并重新设置数据帧格式，使得监控平台可以兼容多种传感器节点。

监控平台采用 C/S 模式或 Web 模式，由数据中心和监控终端（用户端）两部分组成。

数据中心负责原始数据的收集和存储，监控终端（用户端）负责数据的处理和图形化显示。

3.9.1.1 数据中心

数据中心负责数据收集、前期处理和存储。数据中心控制程序通过接口（串口或USB口或以太网接口等）从网关节点收集数据。开始时接口一直处于侦听状态，当有事件触发时，侦听程序便开始从接口读取数据。经过网关节点收集到的原始数据是一系列特定序列的字符串，需要在数据中心进行前期处理及存储。当数据中心接收到原始数据后，首先判断传感器节点和传感器板的类型，然后根据节点程序中设置的数据帧格式，可以知道各感知数据字段在数据包中的位置，利用相应的函数对这些感知数据进行格式转换，提取出所需要的数据。

数据中心采用大型商用数据库（如MySQL）作为后台数据库来对数据进行存储管理，利用其提供的SQL数据控制函数进行操作，存储有效数据，方便用户查询，并具有回放功能。MySQL作为常用的数据库管理系统，功能实用并且查询简单方便，对于开发人员来说很容易掌握，非常实用。

在数据中心，收到的数据包可能来自于不同类型的传感器节点，它们的数据帧格式不同。因此在数据中心对这些数据包统一处理，在数据中增加传感器节点类型字段，然后设置新的数据帧格式。这样，就为监控系统的通用性提供了保障。

当接收到监控终端发送的请求后，按照用户的需求发送数据。监控终端收到数据中心发来的数据后，对收到的数据包进行解析处理，然后显示到监控终端界面。

3.9.1.2 监控终端

当接收到数据中心的数据后，需要对数据进行处理和界面显示。同时对数据和界面进行操作会造成系统阻塞。利用多线程技术，将数据的处理和图形的界面显示分开实现，可以解决系统阻塞问题，它能够可靠地执行并行性任务，并提高了数据处理效率和系统性能，使得界面流畅。界面显示作为主线程，负责维护界面。在程序执行过程中，调用数据处理线程，它们负责各种数据的分析与处理、存储和传送等。

采用模块化设计，使得整个系统层次清晰，可扩展性良好，根据需要进行扩展，具有很大的灵活性。添加新的功能模块，并不需要改变系统的整体框架，并且系统维护简单可靠。

在监控软件的设计中，着重实现了以下3个功能模块：

（1）感知数据表格化显示。系统会收到传感器节点采集的一系列环境数据，例如温度、压力、光强、音频、加速度、位置等各种感知数据，利用表格化实时动态地将这些数据显示出来，使研究人员直观地观察到每个节点的运行状态，从而掌握监控区域小范围内的状态。

（2）网络拓扑结构。实时显示网络中的拓扑结构，同时可以显示节点的路由状态和链路信息，掌握网络运行的整体状态。增加拖动功能，研究人员可以根据自己的需要，在屏幕范围内任意拖动节点位置，方便观察，利于研究。

（3）移动节点跟踪定位。可应用到具体的移动目标节点的定位。根据信标节点传送回

来的位置、距离或者路由跳数等监测数据，采用基于距离的或者与距离无关的定位算法，首先计算出活动目标节点的位置，然后根据合适的目标跟踪算法，采用预测、估计等跟踪技术实现目标节点的定位跟踪。

监控终端软件流程如下：

（1）用户登录，界面初始化；

（2）连接前端服务器控制程序，连接成功后前端服务器向客户端发送数据；

（3）将所有的原始数据信息显示到实时信息输出区；

（4）收到数据包后判断节点类型和传感器板类型；

（5）根据节点类型和传感器板类型建立活动列表，同时将实时数据存入到数据库；

（6）设置定时器，在一定时间段内，如果没有某个节点的数据包到达，说明该节点能耗耗尽或者发生意外情况，将该节点从活动节点列表中删除，但是记录下该节点的活动情况；

（7）在程序界面的左方节点列表区域显示所有活动节点信息；

（8）在感知数据视图、拓扑结构视图和跟踪定位视图中进行动态显示。

3.9.2 无线传感网数据管理

在无线传感网中进行数据管理，有以下几个方面问题：

（1）感知数据如何真实反映物理世界；

（2）节点产生的大量感知数据如何存放；

（3）查询请求如何通过路由到达目标节点；

（4）查询结果存在大量冗余数据，如何进行数据融合；

（5）如何表示查询并进行优化。

因而，无线传感网中的数据管理研究内容主要包括数据获取技术、存储技术、查询处理技术、分析挖掘技术以及数据管理系统的研究。

数据获取技术主要涉及无线传感网和感知数据模型、元数据管理技术、传感器数据处理策略、面向应用的感知数据管理技术。

数据存储技术主要涉及数据存储策略、存取方法和索引技术。

数据查询技术主要包括查询语言、数据融合方法、查询优化技术和数据查询分布式处理技术。

数据分析挖掘技术主要包括分析处理技术、统计分析技术、相关规则等传统类型知识挖掘、与感知数据相关的新知识模型及其挖掘技术、数据分布式挖掘技术。

数据管理系统主要包括数据管理系统的体系结构和数据管理系统的实现技术。

从2002年开始，国际上关于传感器网络中数据管理的研究，就有研究结果发表，主要集中在把数据库技术，尤其是分布式数据库技术和传感器网络技术相结合，实现数据管理。

在传感器网络中对数据进行建模，主要用于解决以下四个问题：

（1）感知数据具有不确定性。节点产生的测量值由于存在误差并不能真实反映物理世界，而是分布在真值附近的某个范围内，这种分布可用连续概率分布函数来描述。传统文献中讨论的数据模型技术大多采用离散概率分布函数，并不能很好地适用于传感器网络。

（2）利用感知数据的空间相关性进行数据融合，减少冗余数据的发送，从而延长网络生命周期。同时，当节点损坏或数据丢失时，可以利用周围邻居节点的数据相关性特点，在一定概率范围内正确发送查询结果。

（3）节点能量受限，必须提高能量利用效率。根据建立的数据模型，可以调节传感器节点工作模式，降低节点采样频率和通信量，达到延长网络生命周期的目的。

（4）方便查询和数据分布管理。

数据存储策略按数据存储的分布情况可分为以下三类：

（1）集中式存储。节点产生的感知数据都发送到基站节点，在基站处进行集中存储和处理。这种策略获得的数据比较详细完整，可以进行复杂的查询和处理。

（2）分布式存储和索引。感知数据按数据名分布存储在无线传感网中，通过提取数据索引进行高效查询。

（3）本地化存储。数据完全保存在本地节点，数据存储的通信开销最小，但是查询效率低下，一般采用泛洪式查询，当查询频繁时，网络的通信开销极大，并且存在热点问题。

无线传感网中的数据查询主要分为快照查询和连续查询。快照查询是对传感器网络某一时间点状况的查询，连续查询则主要关注某段时间间隔内网络数据的变化情况。查询处理与路由策略、感知数据模型和数据存储策略紧密相关，不可分割。当前的研究方向主要集中在以下几个方面：

（1）查询语言研究。这方面的研究目前比较少，主要是基于 SQL 语言的扩展和改进。

（2）连续查询技术。传感器网络中，用户的查询对象是大量的无限实时数据流，连续查询被分解为一系列子查询提交到局部节点进行执行。子查询也是连续查询，需要扫描、过滤、综合数据流，产生部分的查询结果流经过全局综合处理后返回给用户。局部查询是连续查询技术的关键，由于节点数据和环境情况动态变化，局部查询必须具有自适应性。

（3）近似查询技术。感知数据本身存在不确定性，用户对查询结果的要求也是在一定精度范围内的。采用基于概率的近似查询技术，充分利用已有信息和模型信息，在满足用户查询精度要求下减少不必要的数据采集和数据传输，将会提高查询效率，减少数据传输开销。

（4）多查询优化技术。在传感器网络中一段时间间隔内可能进行着多个连续查询，多查询优化就是对各个查询结果进行判别，减少重叠部分的传输次数以减少数据传输量。

3.9.3 典型无线传感网监控 GUI 软件

无线传感网监控软件 V3.00 是一套专门为 C51RF-WSN 开发的无线传感网上位机可视化监控软件，如图 3-117 所示。它基于 .NET 集成开发平台开发而成，因此在使用无线传感网监控软件 V3.00 无线网络监控软件必须安装“Framework Version 2.0.exe”，用户可以在 C51RF-WSN 配套光盘“\ C51RF-WSN 开发软件 \ C51RF-WSN 监控软件”目录下找到，或直接到微软官方网站免费下载。

无线传感网监控软件 V3.00 无线网络监控软件提供网络拓扑可视化显示、传感器节点数据可视化显示（如温度、光敏值、湿度、加速度、信号强度等）、各节点的配置及程序下载、扩展实验的配置，如图 3-118 ~ 图 3-120 所示。

图 3-117　无线网络监控软件界面

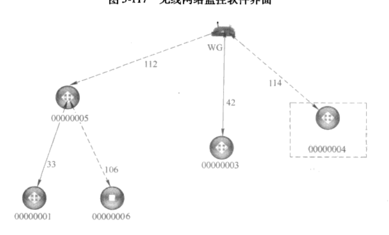


图 3-118　网络拓扑显示

无线传感网监控软件 V3.00 无线网络监控软件的功能特点如下：

(1) 监测并管理传感器网络。

(2) 可视化显示传感器数据。

(3) 网络状况监测。

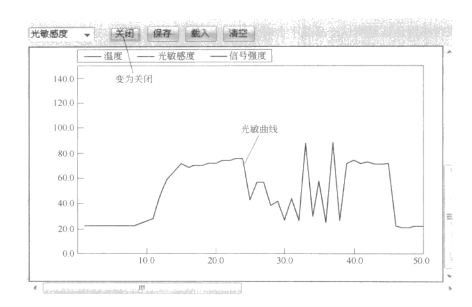


图 3-119 曲线显示图

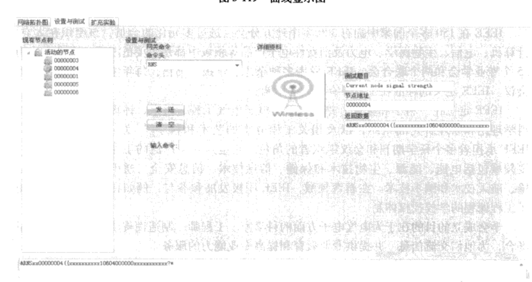


图 3-120 节点管理

（4）发送命令和激励信号。

（5）节点配置功能。

3.10 无线传感网兼容和认证

为了使用不同公司生产、相同技术标准产品能实现可完全互操作及兼容，技术标准组

织需要对其内成员生产、开发产品进行兼容性认证。

无线传感网认证是测试产品或平台对无线传感网标准的兼容性。这种认证是驱使一种新技术成熟化的一个重要环节。没有它，即使企业和消费者声称他们支持相同的认可标准，也不能肯定不同公司的产品是否可以相互操作。

在了解无线传感网认证前，我们先了解一下现在全球有哪些主要无线网络技术标准组织。

3.10.1 全球无线网络技术标准组织

3.10.1.1 电气电子工程师学会

电气电子工程师学会（Institute of Electrical and Electronics Engineers，简称为 IEEE）是一个建立于1963年1月1日的国际性电子技术与电子工程师协会，亦是世界上最大的专业技术组织之一，拥有来自175个国家的36万会员。除设立于美国纽约市的总部以外，其在全球150多个国家拥有分会，并且还有35个专业学会及2个联合会。

1963年1月1日，IEEE 由美国无线电工程师协会（IRE，创立于1912年）和美国电气工程师协会（AIEE，创建于1884年）合并而成，它有一个区域和技术互为补充的组织结构，以地理位置或者技术中心作为组织单位（例如 IEEE 费城分会和 IEEE 计算机协会）。它管理着推荐规则和执行计划的分散组织。

IEEE 在150多个国家中拥有300多个地方分会。透过多元化的会员，该组织在太空、计算机、电信、生物医学、电力及消费性电子产品等领域中都是主要的权威。专业上它有35个专业学会和两个联合会。IEEE 发表多种杂志、学报、书籍，每年组织300多次专业会议。IEEE 定义的标准在工业界有极大的影响。

IEEE 定位在“科学和教育，并直接面向电子电气工程、通讯、计算机工程、计算机科学理论和原理研究的组织，以及相关工程分支的艺术和科学。”为了实现这一目标，IEEE 承担着多个科学期刊和会议组织者的角色。它也是一个广泛的工业标准开发者，主要领域包括电能、能源、生物技术和保健、信息技术、信息安全、通讯、消费电子、运输、航天技术和纳米技术。在教育领域，IEEE 积极发展和参与，例如在高等院校推行电子工程课程的学校授权体制。

学会成立的目的在于为电气电子方面的科学家、工程师、制造商提供国际联络交流的场合，为他们交流信息。并提供专业教育和提高专业能力的服务。

学会的主要活动是召开会议、出版期刊、制定标准、继续教育、颁发奖项、认证（Accreditation）等。IEEE 每年要举办300多个学术会议，有35万人参加。IEEE 的许多学术会议在世界上很有影响，有的规模很大，达到4~5万人。

IEEE 制定了全世界电子和电气还有计算机科学领域30%的文献，另外它还制定了超过900个现行工业标准。每年它还发起或者合作举办超过300次国际技术会议。IEEE 由37个协会组成，还组织了相关的专门技术领域，每年本地组织有规律地召开超过300次会议。IEEE 出版广泛的同级评审期刊，是主要的国际标准机构（现行标准900个，研发中标准700个）。

IEEE 被国际标准化组织授权为可以制定标准的组织，设有专门的标准工作委员会，

有30000义务工作者参与标准的研究和制定工作，每年制定和修订800多个技术标准。

IEEE的标准制定内容有：电气与电子设备、试验方法、元器件、符号、定义以及测试方法等。

A 著名IEEE委员会和格式

IEEE754——浮点算法规范

IEEE802——局域网及城域网

IEEE802.11——无线网络

IEEE829——软件测试文书

IEEE896——未来总线 Futurebus

IEEE1003——POSIX

IEEE1076——VHDL VHSIC 硬件描述语言

IEEE1149.1——JTAG

IEEE1275——Open Firmware

IEEE1284——并口

IEEEP1363——公钥密码

IEEE1394——串行总线“火线”（Firewire）

IEEE1619——存储安全

IEEE12207——信息技术（IT）

B 常见标准

IEEE802.1——高级接口 High Level Interface（Internetworking）

IEEE802.1d——生成树协议（Spanning Tree）

IEEE802.1p——General Registration Protocol

IEEE802.1q——虚拟局域网（Virtual LANs；VLAN）

IEEE802.1x——基于端口的访问控制（Port Based Network Access Control）

IEEE802.2——逻辑链路控制（Logical Link Control）

IEEE802.3——带冲突检测的载波侦听多路访问协议 CSMA/CD（半双工以太网）

IEEE802.3u——快速以太网（Fast Ethernet）

IEEE802.3z——千兆以太网（Gigabit Ethernet）

IEEE802.3ae——万兆以太网（10 Gigabit Ethernet）

IEEE802.4——令牌通行总线（Token-Passing Bus）

IEEE802.5——令牌通行环（Token-Passing Ring）

IEEE802.6——城域网（Metropolitan Area Networks，MAN）

IEEE802.7——宽带局域网（Brandband LAN）

IEEE802.8——光纤局域网

IEEE802.9——集成数据和语音网络（Integrated Voice and Data Networks，VoIP）

IEEE802.9a——IsoENET（proposed）

IEEE802.10——网络安全（Network Security）

IEEE802.11——无线以太网

IEEE802.12——100VG-AnyLAN（Voice Grade - Sprache geeignet）

IEEE802.14——有线电视（CATV）
IEEE802.15——无线个人区域网路（Wireless Personal Area Network，WPAN）
IEEE802.17——弹性分组环（Resilient Packet Ring）

3.10.1.2 蓝牙联盟

Bluetooth™

蓝牙技术始于爱立信公司的1994年方案，它是研究在移动电话和其他配件间进行低功耗、低成本无线通信连接的方法。发明者希望为设备间的通信创造一组统一规则（标准化协议），以解决用户间互不兼容的移动电子设备。1997年前爱立信公司此概念接触了移动设备制造商，讨论其项目合作发展，结果获得支持。1998年项目正式启动。

1999年5月20日，索尼爱立信、IBM、英特尔、诺基亚及东芝等业界龙头创立蓝牙特别兴趣组（Special Interest Group，SIG），制订蓝牙技术标准。蓝牙特别兴趣组本身并不制造、生产或销售蓝牙产品。主要任务是发布蓝牙技术规范，管理认证计划，保护商标。

“蓝牙”这名称来自10世纪的丹麦国王哈拉尔德（Harald Gormsson）的外号。出身海盗家庭的哈拉尔德统一了北欧四分五裂的国家，成为维京王国的国王。由于他喜欢吃蓝莓，牙齿常常被染成蓝色，而获得“蓝牙”的绰号。当时蓝莓因为颜色怪异的缘故被认为是不适合食用的东西，因此这位爱尝新的国王也成为创新与勇于尝试的象征。蓝牙是一个开放性的、短距离无线通信技术标准。它可以用来在较短距离内取代目前多种民缆连接方案，穿透墙壁等障碍，通过统一的短距离无线链路，在各种数字设备之间实现方便、快捷、灵活安全、低成本、小功耗的话音和数据通信。

蓝牙特别兴趣小组（Bluetooth SIG）成立于1998年2月，由以上五个公司宣布成立。到目前为止，已经有超过12000个公司和机构宣布加入蓝牙特别兴趣小组。1999年12月，蓝牙特别兴趣小组正式发布了Bluetooth规范1.0B版，2004年发布了Bluetooth规范2.0版，2009年发布了Bluetooth规范3.0版。

3.10.1.3 ZigBee联盟

ZigBee是一种新兴的短距离、低速率无线网络技术，它是一种介于无线标记技术和蓝牙之间的技术提案。它此前被称作“HomeRF Lite”或“FireFly”无线技术，主要用于近距离无线连接。它有自己的无线电标准，在数千个微小的传感器之间相互协调实现通信。这些传感器只需要很少的能量，以接力的方式通过无线电波将数据从一个传感器传到另一个传感器，所以它们的通信效率非常高。最后这些数据就可以进入计算机用于分析或者被另外一种无线技术如WiMax收集。

ZigBee的基础是IEEE802.15.4，这是IEEE无线个人区域网（Personal Area Network，PAN）工作组的一项标准，被称作IEEE802.15.4（ZigBee）技术标准。ZigBee不仅只是802.15.4的名字。IEEE仅处理低级MAC层和物理层协议，因此ZigBee联盟对其网络层协议和API进行了标准化。

ZigBee 联盟成立于 2001 年 8 月。2002 年下半年，英国 Invensys 公司、日本三菱电气公司、美国摩托罗拉公司以及荷兰飞利浦半导体公司四大巨头共同宣布，它们将加盟“ZigBee 联盟”，以研发名为“ZigBee”的下一代无线通信标准，这一事件成为该项技术发展过程中的里程碑。

到目前为止，除了 Invensys、Ember、三菱电子、摩托罗拉、TI（得州仪器）、飞思卡尔和飞利浦等国际知名的大公司外，该联盟大约已有 200 多家成员企业，并在迅速发展壮大。其中涵盖了半导体生产商、IP 服务提供商、消费类电子厂商及 OEM 商等，例如 Honeywell、Eaton 和 Invensys Metering Systems 等工业控制和家用自动化公司，甚至还有像 Mattel 之类的玩具公司。所有这些公司都参加了负责开发 ZigBee 物理和媒体控制层技术标准的 IEEE802.15.4 工作组。

ZigBee 联盟主要目标是以透过加入无线网络功能，为消费者提供更富弹性、更易用的电子产片。ZigBee 技术能融入各类电子产品，应用范围横跨全球民用、商用、公用及工业用等市场。生产商终于可以利用 ZigBee 这个标准化无线网络平台，设计简单、可靠、便宜又省电的各种产品。

ZigBee 联盟制定网络、安全和应用软件层；提供不同产品的协调性及互通性测试规格；在世界各地推广 ZigBee 品牌并争取市场的关注；管理技术的发展。

3.10.1.4 Wi-Fi 联盟

IEEE802.11 第一个版本发表于 1997 年，其中定义了介质访问接入控制层（MAC 层）和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式，总数据传输速率设计为 2Mb/s。两个设备之间的通信可以自由直接（Ad hoc）的方式进行，也可以在基站（Base Station，BS）或者访问点（Access Point，AP）的协调下进行。

1999 年加上了两个补充版本：802.11a 定义了一个在 5GHz ISM 频段上的数据传输速率可达 54Mb/s 的物理层；802.11b 定义了一个在 2.4GHz 的 ISM 频段上但数据传输速率高达 11Mb/s 的物理层。

2.4GHz 的 ISM 频段为世界上绝大多数国家通用，因此 802.11b 得到了最为广泛的应用。苹果公司把自己开发的 802.11 标准起名叫 AirPort。

Wi-Fi 联盟成立于 1999 年，当时的名称叫做 Wireless Ethernet Compatibility Alliance（WECA）。在 2002 年 10 月，正式改名为 Wi-Fi Alliance。Wi-Fi 联盟致力解决符合 802.11 标准的产品的生产和设备兼容性问题。Wi-Fi 为制定 802.11 无线网络的组织，并非代表无线网络。

Wi-Fi 网络的持续扩张是基于众多的企业、家庭以及现在为人们提供随时随地无线上网地点的公共 hotspot，因此兼容性至关重要。Wi-Fi 联盟制定全球通用的规范，并通过对无线设备的严格测试和 Wi-Fi 认证加以遵循。

迄今为止，Wi-Fi 联盟已经认证了超过 2800 种产品的互操作性。但是，对于 Wi-Fi 联盟而言，还有更多互操作性以外的工作，竭尽全力为 Wi-Fi 用户提供他们对现有的 Wi-Fi 系统做出决断所需要的信息。不管用户是精通技术 IT 主管，具有安全意识的首席信息官，还是被 Wi-Fi 潜在价值所吸引的家庭用户，Wi-Fi 联盟目标就是为用户提供使用他们的产

品所需要的信息，让用户充满信心，且用得放心。

802.11 标准和补充如下：

802.11，1997 年，原始标准（2Mb/s，2.4GHz 频道）。

802.11a，1999 年，物理层补充（54Mb/s，5GHz 频道）。

802.11b，1999 年，物理层补充（11Mb/s，2.4GHz 频道）。

802.11c，符合 802.1D 的媒体接入控制层（MAC）桥接（MAC Layer Bridging）。

802.11d，根据各国无线电规定做的调整。

802.11e，对服务等级（Quality of Service，QoS）的支持。

802.11f，基站的互连性（Interoperability）。

802.11g，物理层补充（54Mb/s，2.4GHz 频道）。

802.11h，无线覆盖半径的调整，室内（indoor）和室外（outdoor）信道（5GHz 频段）。

802.11i，安全和鉴权（Authentification）方面的补充。

802.11n，导入多重输入输出（MIMO）和 40Mb 信道宽度（HT40）技术，基本上是 802.11a/g 的延伸版。

除了上面的 IEEE 标准，另外有一个被称为 IEEE802.11b + 的技术，通过 PBCC 技术（Packet Binary Convolutional Code）在 IEEE802.11b（2.4GHz 频段）基础上提供22Mb/s 的数据传输速率。但这事实上并不是一个 IEEE 的公开标准，而是一项产权私有的技术（产权属于美国得州仪器，Texas Instruments）。也有一些被称为 802.11g + 的技术，在 IEEE802.11g 的基础上提供 108Mb/s 的传输速率，跟 802.11b + 一样，同样是非标准技术，由无线网络芯片生产商 Atheros 所提倡的则为 SuperG。

3.10.2 无线网络产品认证

本节介绍目前两种重要无线网络产品兼容认证。

3.10.2.1 蓝牙认证

蓝牙技术属于一种短距离、低成本的无线连接技术，是一种能够实现语音和数据无线传输的开放性方案，因此无线通信“蓝牙”刚刚露出一点儿芽尖，就已经引起了全球通信业界和广大用户的密切关注。蓝牙技术产品是采用低能耗无线电通信技术来实现语音、数据和视频传输的，其传输速率最高为每秒 1Mb/s，以时分方式进行全双工通信，通信距离为 10m 左右，配置功率放大器可以使通信距离进一步增加。

只有 Bluetooth SIG 的会员才有权将 Bluetooth 的商标使用在商品和服务上。只有通过 Bluetooth 资格认证程序确认的有关 Bluetooth 无线技术的产品和服务，会员才能将商标用在产品和服务上。蓝牙资格认证实验室（BQTF）和蓝牙资格认证专家（BQE）可以协助厂商取得产品的资格认证。

简言之就是如果您的产品具有蓝牙功能并且在产品外观上标明蓝牙标志，必须通过一个叫做 BQB 的认证。蓝牙认证是任何使用蓝牙无线技术的产品所必须经过的证明程序，蓝牙认证团体（BQB）是由蓝牙认证评估委员会（BQRB）授权的，为需要获得蓝牙产品认证的成员提供服务的团体。成员直接通过 BQB 获得认证服务。

BQTF的全称是Bluetooth Qualification Test Facility，蓝牙认证测试工具（BQTF）是经过BQRB正式认可的，能完成测试实例引用列表（TCRL）中的“A类”蓝牙认证一致性测试鉴别。BQTF角色的权威描述在蓝牙认证程序参考文档（PRD）中4.3.3一节。成员可以直接将BQTF用于测试服务。通常BQTF也可以提供额外的蓝牙测试服务。

Bluetooth资格认证局限于下列产品类型的设计：

（1）Bluetooth最终产品。

（2）Bluetooth控制器子系统产品。

（3）Bluetooth主机子系统产品。

（4）Bluetooth配置文件子系统产品。

（5）Bluetooth组件产品。

（6）Bluetooth测试设备。

（7）Bluetooth开发工具。

蓝牙认证是任何使用蓝牙无线技术的产品所必须经过的证明程序。蓝牙系统规范中定义的蓝牙无线技术允许设备间的短距离无线数据连接。

蓝牙认证程序参考文档是产品认证过程的标准参考。

蓝牙特别兴趣组织成员具有特许免费权利在蓝牙认证产品列表（QPL）的产品列表中使用蓝牙无线技术。蓝牙SIG成员是免费的。

蓝牙QPL列出了所有得到许可的蓝牙成品、子系统、组件和开发工具。在QPL中列出的产品是由分布在世界各地的蓝牙认证团体（BQBs）特别授权的。任何BQB都可以评估、认证和列出认证任何产品。及早加入BQB，可使产品开发时间和费用最小化。

蓝牙产品认证方针，在PRD中的文档，是由蓝牙认证评估委员会（BQRB）制定的，该委员会由来自9个蓝牙SIG的发起企业的代表选举产生。认证程序由代表BQRB利益的蓝牙认证管理员（BQA）负责。

BQRB认可个别的蓝牙认证团体（BQBs），授权给他们去认证和列出产品。BQRB也认可那些经过鉴定合格的蓝牙认证测试设备（BQTFs），作为有效的执行和报告A类测试结果（参见认证过程描述获得更详细的信息）。BQRB同样也认可蓝牙技术估价员，由他们来估价和推荐BQTF候选人。

蓝牙认证团体（BQB）是由BQRB授权的，为需要获得蓝牙产品认证的成员提供服务的团体。成员直接通过BQB获得认证服务。BQB负责检查不符合规范的声明和文档，评价产品测试报告，在蓝牙授权产品的官方数据库中列出产品。BQB必须是蓝牙SIG成员或者蓝牙SIG的雇员。BQB是独立的个体，不需要附属于测试工具和生产商。

蓝牙认证测试工具（BQTF）是经过BQRB正式认可的，能完成测试实例引用列表（TCRL）中的“A类”蓝牙认证一致性测试鉴别。BQTF角色的权威描述在蓝牙认证程序参考文档（PRD）中4.3.3一节。成员可以直接将BQTF用于测试服务。通常，BQTF也可以提供额外的蓝牙测试服务。

BQTF的范围包括以下的一个或两个能力范围：

（1）射频一致性测试，包括RF、基带和物理测试规范。

（2）协议和剖面一致性测试，包括基带、链路管理、L2CAP和剖面一致性测试规范。

蓝牙技术评估员（BTA）的任务是代表蓝牙认证评估委员会（BQRB），对委派用于蓝

牙一致性测试及后期由蓝牙 SIG 公司授权的作为蓝牙认证测试设备（BQTF）的测试工具的技术能力进行评估。

指定剖面互操作性测试（DPIT）对于产品互操作性测试非常有用。本页描述 DPITs 选用的处理，包括 Pre-PIT 阶段；同时也描述在执行互操作测试时，在什么样的情况下如何使用 PrePITs 和 DPITs。

现有的 PITs 如下：

（1）Pre-PIT 列表。

（2）DPIT 列表。

DPIT 筛选分为 3 个阶段，即 BQB 评价和 Pre-PIT 列表阶段、PrePIT 评估阶段和最后的 BQRB 评价和决断阶段。

第一个阶段，成员需要加入 BQB 以评估他们的认证产品是否符合 PrePIT 的要求。当所有标准都合格，BQB 将此产品列为 Pre-PIT。

第二阶段，所列的 Pre-PIT 将使用由蓝牙 SIG 成员提供的工具进行测试。成员被邀请评估所列的 Pre-PIT，将通过 BQA（蓝牙认证管理员）向 BQRB 提交肯定或者否定的反馈信息。

接下来是评估阶段，BQRB 将复查列表、测试结果和反馈信息，并考虑是否指定该产品为 DPIT。

在成员请求或 BQRB 最终复查的时候，Pre-PIT 资格也可能会被取消。

下面列出 BQB 在评估阶段认证 pre-pit 必须具备的最低标准条件。

（1）产品至少具有一个蓝牙剖面，符合蓝牙 1.0 规范或者更新的规范以及相应的互操作性测试。

（2）产品必须符合所列出的最终支持的 PRE-PIT 剖面和角色。

（3）产品可以不用包含原先具有的但已放弃的申请认证资格的剖面。

（4）应用鉴别指定的角色和剖面进行测试的适应性，其中“B”类测试已经满足了所提议的 PRE-PIT，这个 PRE-PIT 是经过 BQB 对其他指出产品的成功测试和后来估价所认证而得出的结论。

（5）在测试过程中执行的步骤必须与 Pre-PIT 申请者提供的测试步骤不同。

（6）申请者提供的剖面和剖面角色的用户文档必须符合 pre-pit 的标准要求。

（7）产品对于 DPIT 池就有多样性，例如包括比现存的 DPIT 实现目标剖面所要求的蓝牙组件有所不同。

（8）产品必须保证成员、BQB 和 BQTF 能在 60 天内通过正当的商业途径可以购买得到。

（9）在成员和 BQB 订购产品时必须列出产品所有用到的元器件。

此外，建议成员身份代表应用厂商加入到最近的 UPF 机构。

认证一个 PRE-PIT 之前，在评估产品时 BQB 可以向成员索要产品的技术资料。

有关 PRE-PIT 的所有测试报告和反馈信息，必须提交给 BQB 以备 BQRB 复查。

成员可以要求 BQB 指出一件合格的产品，用于在本节描述的准则下，特定的剖面进行一个预先剖面的互操作测试（“PRE-PIT”）。BQB 声明列出的作为 pre-pit 的产品满足所有的 PRE-PIT 标准。每个 PRE-PIT 列表必须包括以下内容：

（1）所支持的剖面和各个剖面指定的角色（例如客户机、服务器等）。

（2）各个剖面的 PICS（鉴别强制的和可选的实现特征）。

（3）各个满足“B”类测试条件的剖面和剖面指定的角色。

（4）用于 PIT 的文档（覆盖了每个剖面和角色）。

（5）所列出的产品必须通过“B”类测试。

（6）必须明确指出在测试过程中的实现方式不同于 DPIT 的应用方式。

（7）必须包括获得 PRE-PIT 以备复查的具体条款和公司联系方式。

测试成员应当向 Bluetooth SIG 至少提交一个产品用于下面列出的 Pre-PIT 测试要求。作为测试评估的一部分，Bluetooth SIG 将使用机构所指定的测试工具对这个产品进行测试，并且测试过程对成员是免费的。评估完成后，被测试的产品将返回给成员。

鼓励但不要求成员测试所罗列的 PRE-PIT。在列出 PRE-PIT 之后，BQA 将这个列表告知 BTAB 和 BQRB，并要求所有的 BQB 报告记载下四个星期来关于 PRE-PIT 转入 DPIT 的所有信息。例如，记录下其能获得 PRE-PIT 的充分理由。

评估阶段之后，BQRB 必须参考所有的 PRE-PIT 报告。BQRB 可以决定：（1）批准 DPIT；（2）评估公开被关注的未决调查报告；（3）取消产品的 PRE-PIT 资格。BQA 将立即更新产品的资格状态。

关于 Pre-PIT 到 DPIT 状态的更新，如果产品没有向 DPIT 增加有效值或者其他的因素，产品是否符合 DPIT 测试标准等情况，BQRB 具有保留该此产品的否决权。

维持 DPIT 状态的要求如下：

（1）产品必须保持与协议和剖面规范的一致性，包括 TCRL 更新所引入的变动。评估的失败将取消在 DPIT 中已经通过测试单元的 DPIT 资格。如果产品支持多个剖面，其中一个或者多个剖面不匹配，只有那些互相匹配的剖面会被 DPIT 认可。

（2）产品必须具备 DPIT 指出的剖面测试所要求的认证条件。

（3）产品继续给 DPIT 提供有效值。

不符合要求的产品可以不公告就被 BQRB 否决，并从 DPIT 认证列表取消掉资格。

被认为不再为 DPIT 池提供有效值的产品，可以被 BQRB 否决后的一个月内公示取消其资格。

由于可用的 DPIT 剖面不同，互操作性测试要求也可以有所不同。

利用工程学规范剖面所进行的互操作测试。必须用基于工程学的剖面互操作性原则进行测试：测试举证引用表要支持 B 类剖面互操作性测试，并且至少 2 个 DPIT 支持这个剖面。成员将提供一个由 BQB 确定的形式的工程学证明，它支持剖面互操作性要求。这些证明是来源于剖面互操作性测试的也可能包括轨迹或软件设计流程。除提供工程学证明之外，还鼓励成员对于列出产品的互操作性进行测试。用 DPITs 的剖面互操作性测试：产品对产品“互操作性测试（B 类测试）”必须能支持所有应用的蓝牙剖面。在 BQB 指导下，成员选择对互操作性的 DPITs 进行测试，是为了尽量地增加其可选功能的覆盖能力。在每个列出多个 DPITs 的应用剖面中，产品必须至少通过两个 DPIT 测试。如果成员实现了蓝牙系统规范的任一部分可选功能，并且至少一个 DPIT 能够执行相关的互操作性测试，则这个功能性的互操作性测试就能够完成。一个详细描述产品优缺点的测试报告必须在列出列表前提供给 BQB。

在利用 DPIT 进行剖面互操作性测试时会出现如下情况：

（1）B 类剖面互操作性测试存在于测试用例引用列表中，特定剖面存在两个认证了的 DPIT 后。

（2）根据 DPIT 的测试要求，只有在第二次 DPIT 认证之后的 90 天后才可用。

反之，根据 DPIT 的指出，互操作失败不能证明产品不符合蓝牙系统规范。当然，要求成员以别的方式给出其符合规范的证明文档，包括利用 DPIT 的互操作失败的合理解释。不要求成员证明 DPIT 是不符合规范的。

3.10.2.2 Wi-Fi 认证

随着笔记本电脑、掌上 PDA、蜂窝式电话的迅猛发展，人们对这些设备之间互联互通的需求日益增加。目前大部分设备都是基于某种特定的技术规格设计和生产的，它们往往只能和其配套的伙伴产品相互兼容，而无法与其他设备互联互通。为了使各种设备能有效地运行，用户可能会重复地购置一些功能相同的来自不同公司的产品。近来一些公共场所开始提供无线局域网服务，但如果用户使用的无线网卡和这些场所的设施不兼容，就很可能无法享受这些便利的通信服务。

当宽带接入技术与无线局域网相结合时，其速度完全可与标准以太网相媲美。无线部分已不再是网络的瓶颈，任何在 Cable Modem 或 DSL 等宽带接入网上交换的信息流，几乎都可平滑地在无线局域网上传送，例如电子邮件、网上交谈、音频视频流媒体及各种基于 Web 浏览器的应用。

以上这一切都取决于一件事——互操作性，这在无线局域网中是一个尤为突出的问题。没有一个互操作性的标准，哪个产品敢号称能和其他产品完全相通？如果有那么多的设备不能兼容，可以想象世界会变得多么糟糕。

为了解决这个问题，Wi-Fi（Wireless Fidelity 的简称）作为无线局域网互操作性的标准就应运而生了。厂家的产品只有完全满足 Wi-Fi 标准，并通过 Wi-Fi 认证，才可以在其产品上打 Wi-Fi 标签。Wi-Fi 标签是 WECA（无线以太网兼容性联盟）注册的商标，只有通过 WECA 的授权，厂家才可以使用该商标。因此，用户只需认准 Wi-Fi 标签，便可保证他们所购买的无线基站、PC 卡、手持设备、Internet 电话以及其他任何无线局域网产品都能很好地协同工作。

Wi-Fi 认证针对的是基于 IEEE802.11b 标准的无线局域网产品，Wi-Fi 证书是由一个非营利的工业组织即 WECA 颁布的。WECA 是在 1999 年 8 月组建的，到目前为止会员已迅速增加到 150 多个，全球已有 370 个产品获得了 Wi-Fi 认证。WECA 的核心工作是测试和认证。然而，鉴于会员公司之间存在相互竞争，利益冲突难免存在。

为了减小这种冲突，WECA 制定了严格的规章制度和测试与认证的程序。WECA 成立于 1999 年，是一个非营利的组织，目的是对 Wi-Fi 产品进行互操作认证，在全球范围内推广 Wi-Fi——不同市场应用的无线标准。

WECA 一直在研究一套测试手段，以使成员的产品获得认证测试，这样，就可以与其他具有 Wi-Fi 认证的产品进行相互间的通信。当一个产品成功地通过测试，这个公司就获得授权使用 Wi-Fi 商标。

这个测试确保了带有 Wi-Fi 标志的产品将能相互通信。WECA 的成员资格是向所有支

持 Wi-Fi 标准的公司公开的，包括已经是成员的制造商，他们想要提交 Wi-Fi 产品，进行互操作测试。

WECA 全权委托一个独立的第三方组织，即安捷伦科技公司 ICL 互操作性认证实验室(原硅谷网络实验室)，来测试所有会员公司的产品。WECA 并不知道在何时对哪个特定的产品进行测试，也不会被通知哪些产品没有通过测试。只有通过测试并被授予证书的产品才会通知 WECA。

只有 WECA 成员才可以向安捷伦 ICL 实验室递交申请，对其产品进行 Wi-Fi 认证测试。因此，厂家必须先加入 WECA 组织，才能获得 Wi-Fi 测试服务。根据规定，对于同一厂家的不同型号及不同版本的产品都需分别进行测试，OEM 产品需要被再次测试。

为了节省时间和资金，Wi-Fi 测试可分为两个部分——初测和更全面的二级测试。初测的目的是先筛选掉那些远不符合标准的产品，它仅仅只需花几个小时便可完成。对那些连基本的标准都达不到的产品，WECA 不希望花过多时间和资金对它们进行全面测试。

如果产品通过了初测，它会继续经历两天的严格测试。基本的硬件和配置测试是必不可少的：硬件兼容性达标是非常重要的，同时所有的硬件设备还需通过配置的兼容性测试。如果两个设备的设置不匹配，测试也会失败。

WECA 声称，配置问题和硬件本身所引发的兼容性问题一样多。实际上，在 Wi-Fi 认证没有推出之前，从技术角度来看，虽然许多基于 802.11b 的产品是兼容的，但是，当用户把产品买回家以后，就会发现不同厂家对产品的缺省配置并不相同。其结果是，本来兼容的产品也变得不能兼容。虽然这些产品还有协同工作的可能性，但这要求用户得到两家公司的电话技术支持，才能最终解决问题。有了 Wi-Fi 标准的认证，这样的烦琐工作就可以完全避免。

在认证测试中，一些测试是专门针对无线网卡或接入点而制定的，而其他测试需求是所有的硬件都必须满足的。例如，所有通过认证的设备都必须能按特殊的方式来收发信息；必须支持在一定物理范围内的特定数据传输速率；支持加密和未加密的数据；可处理数据包的分段；能在规定的时间范围内，对其他设备做出响应。

测试是采用 NetIQ Chariot 测试软件来进行的，它可以用预定义好的测试程序来模拟特定类型的网络活动。对于 Wi-Fi 测试，有三个主要的测试程序：第一个程序称为 FILESNDL（File Send Long），用来模拟在两个设备之间传送一个大文件；第二个程序称为 INQUIRYL（Inquiry Long），用来模拟一系列客户端、服务器之间的事务处理；第三个程序称为 REALAUD，用来模拟一个组播的 RealAudio 流媒体。

对接入点和无线网卡的测试是分别进行的，它们的测试准则有一些细微的差别。对于接入点和无线网卡的初测主要集中在以下几个方面：是否能正确地连接到网络上；是否能正确地传送大的数据文件；是否能进行客户端/服务器的事务处理；是否能处理流数据。作为兼容性测试，需要利用多个不同厂家的无线网卡对某个接入点进行测试，利用多个不同厂家的接入点对某个无线网卡进行测试。

另外，对无线网卡和接入点也有一些特殊的测试项目。对于无线网卡的特殊测试包括：漫游、数据负荷、广播和组播的接收以及同设置不匹配的接入点的测试。漫游测试用于检验被测站是否能有效地在不同厂家的接入点之间进行切换；数据负荷测试用于检验被

测无线网卡是否能对数据包进行正确的封装；广播和组播包测试则是检验被测站是否能正确接收广播和组播包。接入点的扩展测试包括类似的功能，只是其测试方向同无线网卡测试正好相反。例如，对于无线网卡的漫游测试，主要检验被测站是否能够在不同的接入点之间进行顺利切换；而对接入点的漫游测试，则检验被测接入点是否能够为不同厂家的无线网卡提供漫游服务。

在我国，无线局域网技术和应用正在逐渐兴起，越来越多的厂家开始研制和生产自己的无线局域网产品，网络运营商也开始关注这一市场，并正在进行一些商业试用网的开通试验。但是，Wi-Fi 认证的观念在中国还不太普及，人们还没有充分认识到 Wi-Fi 认证对保证无线局域网顺畅运行的重要性。随着无线局域网的进一步商用化，势必会有更多厂家的产品进入到这一市场。用户应优先选择具有 Wi-Fi 标签的产品，以获得最大可能的产品兼容性保证。

国内的无线局域网设备生产厂家，也可尽早地加入 WECA 组织，使自己的产品通过 Wi-Fi 认证，这样才可以保证在激烈的市场竞争中占据主动。据悉，为方便亚洲国家的无线局域网设备厂家进行 Wi-Fi 认证测试，安捷伦科技公司最近在新加坡成立了全球第四家 ICL 试验室（在此之前，仅在北美有两家，欧洲有一家）。

目前 Wi-Fi 联盟所公布的认证种类如下：

（1）WPA/WPA2。WPA/WPA2 是基于 IEEE802.11a、802.11b、802.11g 的单模、双模或双频的产品所建立的测试程序。内容包含通讯协定的验证、无线网络安全性机制的验证以及网络传输表现与相容性测试。

（2）WMM（Wi-Fi MultiMedia）。当影音多媒体透过无线网络的传递时，要如何验证其带宽保证的机制是否正常运作在不同的无线网络装置及不同的安全性设定上是 WMM 测试的目的。

（3）WMM Power Save。在影音多媒体透过无线网络的传递时，如何透过管理无线网络装置的待命时间来延长电池寿命，并且不影响其功能性，可以透过 WMM Power Save 的测试来验证。

（4）WPS（Wi-Fi Protected Setup）。这是一个 2007 年年初才发布的认证，目的是让消费者可以透过更简单的方式来设定无线网络装置，并且保证有一定的安全性。目前 WPS 允许透过 Pin Input Config（PIN）、Push Button Config（PBC）、USB Flash Drive Config（UFD）以及 Near Field Communication Contactless Token Config（NFC）的方式来设定无线网络装置。

（5）ASD（Application Specific Device）。这是针对除了无线网络存取点（Access Point）及站台（Station）之外其他有特殊应用的无线网络装置，例如 DVD 播放器、投影机、打印机等等。

（6）CWG（Converged Wireless Group）。主要是针对 Wi-Fi mobile converged devices 的 RF 部分测量的测试程序。

3.10.3　典型兼容性认证过程——ZigBee 标准认证过程

ZigBee 联盟认证设备必须经历两类严格的认证流程，这些认证由专业的独立实验室完成并确保设备按照标准工作。这两类认证如下：

（1）ZigBee 兼容平台——通过测试保证无线电模块/微控制器符合联盟规范，并且提供可靠的健壮的无线网络，从而便于 OEM 开发产品。

（2）ZigBee 认证产品——专门为终端用户产品设计的测试过程，保证设备按照承诺工作，使消费者或其他用户放心购买。

什么是 ZigBee 认证呢？就是测试产品或平台对 ZigBee 标准的兼容性。

如果产品有不同的 SKU，并且以除产品或包装的颜色和产品上的名称之外的任何方式来区别的话，那么就需要，它们必须被单独分别测试。如果不恰当的测试，在同一模块中组合使用不同的包装和开发软件可能产生意外的结果。联盟提供产品认证来确保产品像承诺的一样工作，并最终让用户了解它们可以安心购买 ZigBee 产品。

联盟的再次认证文件表明“要求再次认证的修正包括但并不限于任何硬件的改变、软件升级以及形状因素的调整。”改变的装置仅应用于 ZigBee 相关的硬件和软件，或者对用户的产品所作的改变。例如，如果用户保持 PCB 部分和用于支持 ZigBee 的软件不变，但对用户应用中的其他部分作改变，那会因为这一变化而使得整个系统需要做再次认证么？

如果这是一个新的 SKU，那么是的。再次测试的范围正比于改变的范围。如果变化正如上面所说的那样，测试应该很少并且费用很低。

什么是 ZigBee 认证标识？这与 ZigBee 标识不同么？如果一款产品没有认证，可以用什么文件来使用 ZigBee 标识？那是基本的 ZigBee 标识“红色圆形 Z”连同单词 ZigBee（可以获得的技术）。使用 ZigBee 名称或标识的产品必须进行认证。

ZigBee 认证是必需的吗？其费用是多少？如何完成它？如果计划使用 ZigBee 标识和名称来销售产品，那么认证就是必需的。除 ZigBee 兼容平台认证测试之外，更多的涉及产品自身功能，ZigBee 认证产品测试会是相对简单的，而且费用很低。为了确保竞争，ZigBee 目前已经授权两家试验室进行测试。

仅仅那些成员公司希望使用 ZigBee 名称和标识，并且从联盟的销售项目中获益的产品才要求认证。联盟不会促销未认证产品，并且该产品不可以使用 ZigBee 名称和标识。

如果想获得 ZigBee 认证，那么首先要成为 ZigBee 成员中的一员。ZigBee 认证步骤如下：

（1）加入 ZigBee 联盟。成功加入 ZigBee 联盟，履行 ZigBee 联盟协议并交纳年费。

（2）申请认证。ZigBee 成员申请 ZigBee 认证，了解并遵守认证审查政策、程序及认证指南，正确填写申请认证表。

（3）提交产品测试。ZigBee 成员选择一家 ZigBee 联盟授权试验室测试其提供的产品。产品测试有两个作用：1）确保产品符合 ZigBee 技术规格。2）确保具有产品合格兼容。

（4）通过测试。ZigBee 联盟授权试验室通知 ZigBee 联盟成功地完成了认证测试。通知不包括测试结果或机密资料，只有一般“通行证”声明。

（5）提供认证文书。认证申请成员提供适当产品及测试文件。

（6）确定成员身份。ZigBee 联盟确定认证申请成员的 ZigBee 成员身份，确定其是履行 ZigBee 联盟协议并交纳年费的良好信誉成员。

（7）ZigBee 联盟审查和核准。ZigBee 联盟获得实验室测试结果，5 个工作日之内进行

审查，并提供认证徽标使用权。

（8）审计。ZigBee 检查以确保提交认证资料（应用、一致性声明和测试结果）符合产品认证要求。

（9）通知。ZigBee 将向各会员通知审计结果，如果结果是成功的，ZigBee 联盟将颁发证书，并将该产品写入注册认证产品目录；如果审计结果表明不符合要求，申请成员可做出更正，并重新申请。

（10）认证标识。ZigBee 认证产品标识适用成功完成认证的终端产品。

第4章 现代无线传感网系统设计实例

本章通过几个经典实例来介绍现代无线传感器网络系统设计过程。

4.1 家庭自动化系统设计实例

家庭自动化是指利用微处理电子技术来集成或控制家中的电子电器产品或系统。例如：照明灯、咖啡炉、电脑设备、保安系统、暖气及冷气系统、视讯及音响系统等。

家庭自动化系统主要是以一个中央微处理机接收来自相关电子电器产品的信息（外界环境因素的变化，如太阳初升或西落等所造成的光线变化等）后，再以既定的程序发送适当的信息给其他电子电器产品。中央微处理机必须透过许多界面来控制家中的电器产品，这些界面可以是键盘，也可以是触摸式荧幕、按钮、电脑、电话机、遥控器等。消费者可发送信号至中央微处理机，或接收来自中央微处理机的讯号。

家庭自动化的用途极广，例如当一个人在冬天从外面归来，只要靠近房子，感应器因侦测到人体移动而发出的讯号，会自动打开门前的照明灯，并启动家中的暖气系统；又如早上7点起床，家中的电子时钟发出讯号，让咖啡炉自动煮咖啡，卧室的窗帘自动打开，镭射音响自动演奏优美的旋律等。这一切生活中的方便在美国已经成为现实，并随着互联网的普及逐渐渗入了我国百姓的生活，上网已开始成为多数人一项迫不及待的需求。

不管您想要完成的是什么样的自动化，都需要一个公共网络，以便把各种各样的设备连接于系统之中。网络可采用硬线连接、软线连接、无线连接或这些连接方式的组合。目前，大多数的家庭控制网络采用的都是硬线连接，有专用电缆与CPU相连。一般都认为这是最为可靠的方法，但它需要在房间里进行大量的电缆布线工作，因此硬线连接法往往只是在新建房屋或进行大规模房屋整修时被选用。通过一个简单网关系统即可实现家庭网络与互联网连接，实现远程监控，在办公室里、机场、车站、酒店等随时随地监控家庭状况。

对于那些难以在墙内埋设专用电缆的多数家庭而言，可采用ZigBee无线网络技术。ZigBee联盟目前积极推广的市场包括家庭自动化（Home Automation）、商业大楼自动化（Building Automation）与自动读表系统（Automatic Meter Reading）。

无线连接的优势是多方面的，主要表现在以下几个方面：

（1）无线家庭网络连接不需要在墙上穿洞，也不需要敷设昂贵的光缆，用户很快就能够使用；

（2）使便携式设备能够保持其便携性，不必固定在墙上，且仍可与网络中的其他设备进行通信；

（3）大多数无线网络都采用了某种形式的加密，为用户提供了保密性；

（4）在大多数情况下，无线设备的室内通信距离可达1～100m左右（室外可达1000m以上）。

无线智能照明系统的控制器与照明灯节点之间只需传输开关信号和调光信号等开光量，且数据发送频率不高，而 ZigBee 的最大传输速率可以达到 250 kb/s，这对于实现无线智能照明系统来说已经足够；智能照明系统需要系统具有穿墙的信号传递功能和网络功能，ZigBee 工作在 2.4GHz 的 ISM 频段，信号具有一定的穿墙能力，并且 ZigBee 支持路由节点，只要合理布局，可以保证建筑物内没有无线通信的盲区，这是红外技术所无法提供的。

ZigBee 的两个节点之间的一次数据发送过程在 5 ms 之内即可完成，满足照明系统对实时性的要求；照明系统对成本非常敏感，这将决定它能否实用化和产业化，ZigBee 是一种低速率、低成本的无线通信技术，相比于 Wi-Fi 和 UWB 等这些适用于无线局域网和多媒体应用的高速率无线标准而言，成本非常低廉。本文主要讨论基于 ZigBee 技术的无线智能照明系统的软硬件设计。

4.1.1　基于 ZigBee 的智能照明系统实现

ZigBee 是一种基于 802.15.4 在无线个人网络领域中新兴的无线网络技术。ZigBee 联盟推出 ZigBee 最新规范 ZigBee2007/PRO。

目前 ZigBee 标准在 ZigBee 联盟的推动下正日趋增强和完善，其中 TI 公司 CC2430 加 Z-Stack 协议栈是业内公认最成熟的解决方案。本节的无线智能照明系统就是在这个平台上实现的。

无线智能照明系统的网络节点分为协调器、路由器和终端节点三种。其中，协调器的硬件结构如图 4-1 所示。

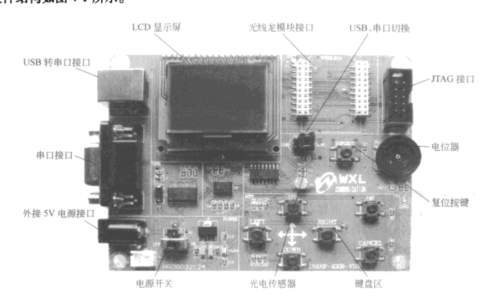


图 4-1　协调器硬件结构

CC2430 芯片是首款符合 ZigBee 技术标准的系统单芯片，片内集成增强的 8051 微控制器内核和符合 IEEE802.15.4 标准的 2.4GHz 射频收发器，具有优良的无线接收灵敏度和强大的抗干扰性能，处于休眠模式时整个芯片的流耗小于 0.9μA，从硬件上支持 CSMA/CA

机制，还集成有 ADC、AES 安全协处理器和 USART 等片上外设及丰富的 I/O 口资源。

只需添加晶振等少量的元器件即可完成 ZigBee 节点的设计。协调器节点带有 44 的键盘，用来设置整个系统的参数和发送控制命令，128×64 汉字图形点阵液晶模块用于显示网络状态信息。微控制器输出开关量直接完成对照明灯的开关控制，微控制器输出的数字量经过 8 位的数/模转换器后，可以实现对照明灯的 256 级调光控制。

另外协调器节点还带有震动感测器和亮度感测器，用于感测现场的震动信息和亮度信息。当震动感测器测得震动较弱，即认为现场人员已经离开，此时可以自动关掉照明灯或者调暗亮度。

当亮度感测器测得光线太亮，如晴朗的白天，即可自动调低亮度；当亮度感测器测得光线太暗，如夜晚或者阴雨的白天，即可调高亮度。系统只需在一个节点上集成震动感测器和亮度感测器，即可通过 ZigBee 网络向各个灯节点传输控制信息，实现对整个照明系统的智能控制，成本低廉。当然也可以将震动感测器和亮度感测器做成一个单独的 ZigBee 网络节点，用于感测现场不同位置的震动信息和亮度信息。

软件设计基于 TI 公司推出的跟 CC2430 芯片配套 Z-Stack 协议栈和 IAR 集成开发环境。Z-Stack 在业内处于领先水平，目前还在不断完善和增强，其最新版本 Z-Stack 1.4.3 已通过 ZigBee 测试机构德国莱茵集团 ZigBee 兼容性测试，符合 ZigBee 2006，已被全球众多 ZigBee 应用开发厂家所采用，支持多种硬件平台，包括面向 IEEE/ZigBee 的 CC2430 片上系统解决方案，基于 CC2420 收发器的新平台和 MSP430 超低功耗微处理器。此外，Z-Stack还支持丰富的新特性，如无线下载，即通过 ZigBee 网络，下载网络中各节点的升级软件，完成节点的软件升级。Z-Stack 还支持具备定位感知功能的 CC2431，该特性使用户能够设计出可根据节点当前位置改变节点行为的新型 ZigBee 应用。

针对 ZigBee 在家庭网络方面的应用，ZigBee Alliance 制定专门的应用框架，即 ZigBee Home Automation Public Application Profile。所谓 Profile 是对逻辑设备及其接口的描述集合，是针对某个特定应用的公约和准则，其目的是使不同厂家按照同一个 Profile 设计的产品之间可以相互操作、相互替换。ZigBee HomeAutomation Public Application Profile 规定了智能家居中的照明设备、采暖通风空调设备、自动窗帘和报警装置的设计规范。本节的无线智能照明系统就是在这个 Profile 的基础上实现的。

Z-Stack 提供了丰富的函数调用接口。

发送数据通过在应用层调用 void SampleApp_SendFlashMessage(uint16 flashTime)函数完成，其中 flashTime 为发送的数据（此函数可以根据不同需要修改相应的函数）。这个函数在应用中通过调用 afStatus_t AF_DataRequest(afAddrType_t * dstAddr, endPointDesc_t * srcEP, uint16 cID, uint16 len, uint8 * buf, uint8 * transID, uint8 options, uint8 radius)函数完成数据的发送。

```
afStatus_t AF_DataRequest( afAddrType_t * dstAddr,          //发送类型
                           endPointDesc_ t * srcEP,         //目的地址
                           uint16 cID,                      //串 ID
                           uint16 len,                      //有效数据长度
                           uint8 * buf,                     //数据
                           uint8 * transID,                 //传输序列号
```

```
                    uint8 options,                        //传输选项
                    uint8 radius)                         //路由深度
```

接收数据通过在应用层调用 void SampleApp_MessageMSGCB(afIncomingMSGPacket_t * pkt)函数完成，其中 * pkt 为接收的数据，在这个函数前，硬件已经将数据接收完成，并存放在 buffer 中。这个函数是通过取 buffer 中的数据来实现相应的功能，如下面的程序清单所示：

```
/********************************************************************************
//函数名:void SampleApp_MessageMSGCB(afIncomingMSGPacket_t * pkt)
//功能：接收数据
//输入：接收的数据
//输出：小灯闪烁的时间
********************************************************************************/
void SampleApp_MessageMSGCB(afIncomingMSGPacket_t * pkt)
{
  uint16 flashTime;
  switch(pkt- > clusterId)                               //判断串 ID
   {
  case SAMPLEAPP_PERIODIC_CLUSTERID:                     //周期发送 ID
    break;
  case SAMPLEAPP_FLASH_CLUSTERID:                        Flash 发送 ID
    flashTime = BUILD_UINT16(pkt- > cmd. Data[1],pkt- > cmd. Data[2]);
    HalLedBlink(HAL_LED_4,4,50,(flashTime/4));           //小灯闪烁
    break;
  }
}
```

在一个两室两厅的套房中布置 1 套基于 ZigBee 技术实现的无线智能照明系统的实验网络，其网络结构如图 4-2 所示。

在每盏灯中都集成有 ZigBee 模块，其中协调器节点是必需的。在其他地方，根据是否需要路由功能，可以配置为路由器或者终端节点。因为协调器节点和路由器节点具有路由功能，协议栈容量较大，所需的 FLASH 空间较大，芯片的成本也较高，因此只把需要给其他节点路由转发数据包的节点配置为路由器节点，其他节点则都配置为终端节点，以降低成本。

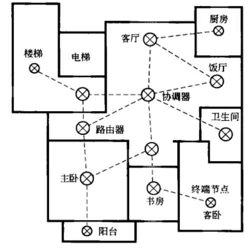


图 4-2　无线智能照明系统网络结构

室内所有的照明灯组成一个 ZigBee 网络，由协调器完成对所有照明灯的控制。可以对网络中的照明灯单个分别进行控制，也可以把所有的照明灯作为一个整体，进行同时控制；实现了对照明灯的简单开关控制和

256 级的调光控制；既可以设置成手动控制模式，也可以设置成自动控制模式，由协调器根据亮度感测器和震动感测器返回的亮度信息和震动信息，自动发送控制命令，完成对所有照明灯的控制。系统设计成本低廉、可靠性高、响应速度快、智能化程度高，是不断发展的电子信息技术在照明领域中的应用，必将带来照明技术的革新。

主函数程序清单如下所示：

```
/***********************************************************************
//函数名:ZSEG int main(void)
//功能:主函数初始化设备、进入操作系统
//输入:无
//输出:无
***********************************************************************/
ZSEG int main(void)
{
  //关闭所有中断
  osal_int_disable(INTS_ALL);
  //确认电压充足才开始运行
  zmain_vdd_check();
  //初始化闪存
  zmain_ram_init();
  //初始化 I/O
  InitBoard(OB_COLD);
  //初始化设备
  HalDriverInit ();
  //初始化 NV 系统
  osal_nv_init(NULL);
  //确定扩展地址
  zmain_ext_addr();
  zgInit ();
  //初始化 MAC
  ZMacInit ();
#ifndef NONWK
  //Since the AF isn't a task, call it's initialization routine
  afInit ();
#endif
  //初始化操作系统
  osal_init_system();
  //允许中断
  osal_int_enable(INTS_ALL);
  //最终硬件初始化
  InitBoard(OB_READY);
  zmain_dev_info();
#ifdef LCD_SUPPORTED
```

```
  zmain_lcd_init();
#endif
  osal_start_system(); //进入操作系统
}
```

随着经济的发展，能源将制约我国经济的发展，因此节能的意义巨大。这种无线控制方式灵活、方便，无需考虑控制布线问题，维护简单。基于ZigBee技术的无线智能系统对节约电能的消耗也起到了很大的作用，符合国家节能减排的发展战略。

4.1.2 基于GPRS/ZigBee的智能家居控制系统

以飞思卡尔MC13224为核心，ZigBee控制芯片构建内部ZigBee无线传感器网络，凭借无线龙科技ARM9嵌入式网关的优越性能，搭建了家庭智能管理平台，设计了一种智能家居控制系统，用户通过GPRS手机或互联网等无线接入技术来访问家庭内部网络，实现了用户对家居环境的智能无线监控、远程查询、集中管理和控制。

随着国民经济和科学技术水平的提高，特别是计算机技术、通信技术、网络技术、控制技术的迅猛发展与提高，促使家庭实现了生活现代化，居住环境舒适化、安全化。这些高科技已经影响到人们生活的方方面面，改变了人们生活习惯，提高了人们生活质量，家居智能化也正是在这种形势下应运而生的。

家庭智能控制系统通过家庭总线技术，构成一个完整的集家庭通信、家庭设备自动控制、家庭安全防范等功能的控制系统，把家庭中各种家用电器、家庭保安装置和各种计量设备连接到一起组成一个家庭内部网络，由家庭智能控制器进行统一管理。

智能家居控制系统凭借各种检测设备来收集外界数据，将收集的数据通过ZigBee无线传感网交给以ARM为核心的嵌入式系统网关进行处理和运算，通过ZigBee无线传感网管理和控制各控制终端，并进行处理、自动控制和调节。

下面介绍ZigBee无线传感网涉及的包括数据收发在内的函数功能和实验的总体功能描述，如以下程序清单所示：

```
/************************************************************************
//函数名:void osalAddTasks(void)
//功能:操作系统添加任务
//输入:无
//输出:无
************************************************************************/
void osalAddTasks(void)
{
/*这个任务必须首先加载,因为Hal_Init()要初始化一些必须的任务初始化函数*/
  osalTaskAdd(Hal_Init,Hal_ProcessEvent,OSAL_TASK_PRIORITY_LOW);
#if defined(ZMAC_F8W)
  osalTaskAdd(macTaskInit,macEventLoop,OSAL_TASK_PRIORITY_HIGH);
#endif
#if defined(MT_TASK)
  osalTaskAdd(MT_TaskInit,MT_ProcessEvent,OSAL_TASK_PRIORITY_LOW);
```

```
#endif
  osalTaskAdd(nwk_init,nwk_event_loop,OSAL_TASK_PRIORITY_MED);
  osalTaskAdd(APS_Init,APS_event_loop,OSAL_TASK_PRIORITY_LOW);
  osalTaskAdd(ZDApp_Init,ZDApp_event_loop,OSAL_TASK_PRIORITY_LOW);
  //SampleApp 的主要任务
  osalTaskAdd(SampleApp_Init,SampleApp_ProcessEvent,OSAL_TASK_PRIORITY_LOW);
}
```

上面是本实验中所有的任务列表，在这里，将只对应用层 SampleApp_ProcessEvent 任务进行分析，下面是 SampleApp_ProcessEvent 函数的源代码：

```
/*********************************************************************/
//函数名:uint16 SampleApp_ProcessEvent(uint8 task_id,uint16 events)
//功能：一般请求任务事件处理器. 这个函数是调用处理所有时间任务，时间包括时间、信息和所有其
       他使用者定义的事件
//输入：操作系统反派的任务 ID、事件的处理
//输出：无
/*********************************************************************
uint16 SampleApp_ ProcessEvent (uint8 task_ id, uint16 events)
{
    afIncomingMSGPacket_t * MSGpkt;
    if(events & SYS_EVENT_MSG)
     {
    MSGpkt = (afIncomingMSGPacket_t * )osal_msg_receive(SampleApp_TaskID);
    while(MSGpkt)
    {
        switch(MSGpkt->hdr.event)
    {
        //按键触发事件
        case KEY_CHANGE:
          SampleApp_HandleKeys(((keyChange_t * )MSGpkt)->state,
                               ((keyChange_t * )MSGpkt)->keys);
          break;
    //接收数据事件
    case AF_INCOMING_MSG_CMD:
    SampleApp_MessageMSGCB(MSGpkt);
    break;
    //设备状态变化事件
    case ZDO_STATE_CHANGE:
      SampleApp_NwkState = (devStates_t)(MSGpkt->hdr.status);
      if((SampleApp_NwkState == DEV_ZB_COORD)
            ||(SampleApp_NwkState == DEV_ROUTER)
            ||(SampleApp_NwkState == DEV_END_DEVICE))
    {
```

```
        //在一个时间间隔中周期性发送一个数据。
        osal_start_timerEx( SampleApp_TaskID,
                            SAMPLEAPP_SEND_PERIODIC_MSG_EVT,
                            SAMPLEAPP_SEND_PERIODIC_MSG_TIMEOUT) ;
      }
      else
      {
        }
      break;
      default:
        break;
      }
      //释放 Flash
      osal_msg_deallocate( ( uint8 * ) MSGpkt) ;
      //如果有一个是可以用的
      MSGpkt = ( afIncomingMSGPacket_t * ) osal_msg_receive( SampleApp_TaskID) ;
      }

      //返回没有处理的事件
      return( events ^ SYS_EVENT_MSG) ;
  }
  //发送一个数据出去：这个任务是产生一个时间
  if( events & SAMPLEAPP_SEND_PERIODIC_MSG_EVT)
   {
  //发送一个周期信息
  SampleApp_SendPeriodicMessage( ) ;
  osal_start_timerEx( SampleApp_TaskID,SAMPLEAPP_SEND_PERIODIC_MSG_EVT,
    (SAMPLEAPP_SEND_PERIODIC_MSG_TIMEOUT + ( osal_rand( ) & 0x00FF) ) ) ;
      return( events^SAMPLEAPP_SEND_PERIODIC_MSG_EVT) ;
  }
  //丢掉没有定义的事件
  return 0;
  }
```

在上面的程序中不难发现，在这个任务中一共存在按键、接收数据和设备状态转变三个事件。如果按键事件则通过键盘实现相应的操作（按键在网络扩展板中）；接收数据事件是完成一次数据接收后对数据的处理。下面一段为按键扫描函数：

```
/**********************************************************************
/函数名:void SampleApp_HandleKeys( uint8 shift,uint8 keys)
//功能：通过按键完成人机通信，当按键 1 按下将发送一组数据。
//输入：扫描到的按键值
//输出：无
*********************************************************************/
```

```
void SampleApp_HandleKeys( uint8 shift,uint8 keys)
{
  if( keys & HAL_KEY_SW_1)
  {
  SampleApp_SendFlashMessage( SAMPLEAPP_FLASH_DURATION);
  }
  if( keys & HAL_KEY_SW_2)
  {
      }
    }
```

发送函数程序清单如下所示:

```
void SampleApp_SendFlashMessage( uint16 flashTime)
{
  uint8 buffer[ ] = "Thank You!";//发送的数据
  if( AF_DataRequest( &SampleApp_Flash_DstAddr,&SampleApp_epDesc,
          SAMPLEAPP_FLASH_CLUSTERID,
          10,                              //数据长度
          buffer,
          &SampleApp_TransID,
          AF_DISCV_ROUTE,
          AF_DEFAULT_RADIUS) == afStatus_SUCCESS)
  {
  }
  else
  {
  }
}
```

接收函数程序清单如下所示:

```
void SampleApp_MessageMSGCB( afIncomingMSGPacket_t * pkt)
{
  switch( pkt- > clusterId)
  {
  case SAMPLEAPP_PERIODIC_CLUSTERID:
      break;
    case SAMPLEAPP_FLASH_CLUSTERID:
    HalLedBlink( HAL_LED_4,4,50,(1000/4));
    break;
  }
}
```

以 ARM 为核心的嵌入式系统将其经过处理的数据通过 RS232 串口通信及时交给 GPRS 模块, GPRS 模块发射和接收无线信号来为外部提供网络接口, 连通家庭内部网络和外部

互联网，使得用户可以通过 GPRS 手机或互联网等方式来访问家庭内部网络，实现远程监视和控制。

系统带有 LCD 和键盘，具有良好的人机界面，方便用户实现本地控制，还可以通过键盘来设定系统的任务；系统留有丰富的功能扩展接口，通过这些扩展接口将来还可以实现家电控制、安防和智能抄表等应用。智能家居控制系统实现的具体功能包括：（1）家用设备的数据采集、处理和反馈。（2）本地控制。用户通过控制系统上的键盘和显示屏，对家用设备进行监控。（3）远程控制。用户可以发送手机短信或通过互联网对家庭系统进行查询和控制。（4）自动报警。当检测到非法闯入或温度超高等报警信号时，及时触发室内报警装置，并通过发送报警短信等方式及时通知用户。（5）温度查询。（6）防盗门密码设置。（7）红外加电控制。（8）灯具等开关量控制。（9）“三表”远程自动抄送与门禁功能。

智能家居控制系统的硬件主要由网关 ARM9 嵌入式控制器、ZigBee 模块、GPRS 模块、键盘/LCD、电源、外设状态检测及控制模块、报警装置、外部扩展的 SDRAM 和 FLASH 组成。其中，控制系统的主控芯片采用 ARM912，使用 ARM9 核，经过串口扩展与 GPRS 模块相连，用户通过 GPRS 手机或互联网等无线接入技术来访问家庭内部网络，实现了用户对家居环境的智能无线监控、远程查询、集中管理和控制。ZigBee 模块通过电平转换芯片提供串口总线接口与家用设备相连接，收集和处理家用设备的相关数据；键盘/LCD 交互接口，方便用户与控制系统间的对话；电源管理接口提供工作电源；报警装置为用户提供报警信息。外设状态检测及控制模块可以对受控终端自动完成信息采集等工作，并能够根据主控模块的命令改变受控终端的状态。系统工作时，监控终端循环检测安装在室内的门磁、红外、烟雾、燃气监测等传感器，当检测到有异常情况发生时，终端控制警笛发出告警声音，提醒户主及物业管理人员有险情发生并采取防范措施，完成家电控制、安防、抄表控制等功能。系统结构框图如图 4-3 所示。

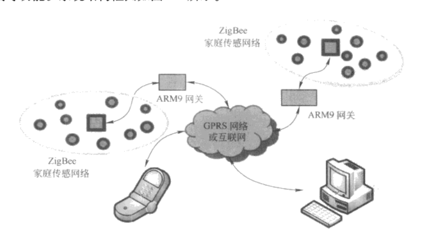


图 4-3　智能家居控制系统结构

监控中心的功能是实现信息的接收和保存。设计语言采用 .NET 的 Visual C#编程语言，它支持网络编程和数据库。监控部分可以直接访问互联网。监控中心只需通过中心软

件侦听网络，接收无线模块传来的 UDP 协议 IP 包和发送上位机控制信息，以实现与终端的 IP 协议通信。接收到的信息要保存到中心的数据库中，以备查历史记录。数据库采用 MSSQL、VC#编制的界面窗口，通过 ADO 访问 MSSQL 中的数据。Socket 接口是 TCP/IP 网络的 API，Socket 接口定义了许多函数和例程，程序员可以利用它来开发 TCP/IP 网络上的应用程序。VC#中的 MFC 类的 CAsyncSocket 这个套接字类，用它来实现 Socket 编程非常方便。设计中采用数据报文式的 Socket，对应于无连接的 UDP 服务应用。CAsyncSocket 类用 DoCallBack 函数处理 MFC 消息，当一个网络事件发生时，DoCallBack 函数按照网络事件类型（FD-READ、FD-WRITE、FD-ACCEPT 和 FD-CONNECT）分别调用 OnReceive、On. Send、OnAccept 和 OnConnect 函数，驱动相应的事件，完成网络数据通信过程，实现系统参数设置、操作员权限管理、用户管理、告警事件处理、数据库的维护以及数据打印和系统帮助等功能。

4.1.3 ZigBee 在家庭自动化中的应用

家庭内部通常地理范围较小，而无线通信具有无需进行铺线等有线通信所不具备的优势，因此家庭网络中的联网非常适合通过近距离无线通信来实现。为了把人们从日常琐事中解放出来，家庭自动化是 ZigBee 技术最有吸引力的一种应用。有了 ZigBee 之后，尽管家里的电器来自不同厂家，但它们都能彼此沟通和合作。

可以如此配置家庭网络：当打开电视机时，灯光自动减弱；当电话铃响起时或拿起话机准备打电话时，电视机自动静音。利用 Zigbee 技术还可以做更多的事，例如家里的每一个成员都可以有一个私人的电子轮廓（它可能是一个小小的符合 Zigbee 标准的器件），其他电器都可以通过检测此轮廓而有所反应。现在，假如附近没有其他轮廓或者某个人的轮廓具有最高优先级，那么家里的灯光、温度、音乐、电视节目和网站都将自动按照这个人的喜好自动设置。如果把私人轮廓放在口袋里，还可以把自动化带到室外或办公室里。为了让轮廓达到上述效果，并不需要完成复杂的配置，因为轮廓可以通过自学程序自动构成。

家庭网络通过家庭网关与电信网络相结合，可以让用户使用手机、电话或互联网随时随地了解到家中出现的任何状况，对家中的电器进行远程控制和操作。

当前的高级家庭自动化系统要求电器智能元件具备超低功耗特性、协同工作能力和网络功能。家庭自动化成为 ZigBee 技术的一个关键应用，应该归功于 ZigBee 的低功耗、互操作功能。飞思卡尔的解决方案是 ZigBee 兼容，并为系统等产品提供与住宅中的其他设备互操作的功能。使用家庭自动化系统，房主能够通过电话或互联网远程控制家庭装置的诸多功能。ZigBee 家庭自动化系统可以节约能源，还能管理一些日常预定任务，包括运行水池水泵和灌溉系统、检查和调节温度与照明系统。ZigBee 家庭自动化系统可以通过电话、短消息（SMS）和网络向房主发出关于入侵、烟火探测、告警状态的通知，从而将家庭安全性提升到一个新的水平。ZigBee 的另一优势在于该类产品可以联网，同时还具有高可靠及高安全等特性。ZigBee 网络可在烟雾探测器和其他系统间进行信号路由。因此，发生火灾时，某一个烟雾传感器的报警会触发整个楼宇内其他烟雾传感器的报警，同时自动开启洒水系统和应急灯，大厦管理人员还能迅速知晓哪里是火灾源头。

美国伊顿（Eaton）推出了采用近距离无线通信标准 ZigBee 的家用传感器产品。

ZigBee家用传感器产品主要通过提示用户家中的电器产品、门窗等的状态来确保安全。比如，可以在出门前确认家中的窗户是否已全部关好，或者咖啡机等电器是否已经关闭等。ZigBee 家用传感器产品由传感器、存储信息的“Base Station”和通过液晶屏显示信息的便携式“HomeKey”组成，均具备基于 ZigBee 的通信功能。传感器方面，备有用于检测管道漏水、确认门窗状态以及电源开关状态的产品。为了便于用户单手操作，ZigBee 家用传感器产品采用了可用大拇指滚动画面的设计。另外 ZigBee 家用传感器产品还具有网络接入设备认证功能。在初次使用时，用户只要将 HomeKey 插入 Base Station 后，再将 HomeKey 插入设置在家中各处的传感器，即可构成网络。

韩国最大的电信公司在 2005 年 10 月推出了新的数字智能家庭服务，其核心的技术为 Ember 公司提供的 ZigBee 无线技术。该服务可以使用户采用手机、互联网遥控家庭设备。第一阶段，数字家庭服务将提供 Ember 公司无线设备、传感器和服务，用于监视和控制家用设备、电灯、烟雾探测器、防盗探测器、室温控制器、气体阀门和电子门锁，所有连接通过基于 ZigBee 技术的网关无线连接到互联网。用户可以通过远程或在家内采用家庭监控服务监测和控制这些设备。

家庭内部通常地理范围较小，而无线通信具有无需进行铺线等有线通信所不具备的优势，因此家庭网络中的联网非常适合通过近距离无线通信来实现。ZigBee 技术具备的超低功耗特性、协同工作能力和网络功能使得它相当适合担当家庭自动化领域中的主要角色。ZigBee 在家庭网络中起到的作用主要表现在以下四个方面：

（1）控制。享受灵活的管理方式，可以从家里的任何地方控制电灯、暖气、空调系统；多个家庭系统的自动控制，使生活更加节能、方便、安全。

（2）节能。获取详尽的电、水、煤气使用数据；嵌入的智能系统能够优化对自然资源的消耗。

（3）便利。不需布线就可以安装、升级网络化的家庭控制系统；从一个单一控制远端就可以配置和运行多个系统。

（4）安全。安装方便的无线传感器能够在多种环境中进行监控；检测到异常事件时能自动接收到系统提示。

我国的家用无线自动控制系统市场正在兴起，而 ZigBee 将在其中扮演重要角色。ZigBee 实现的智能家庭将使我们的生活更加节能、方便、安全、舒适。可以预见在不远的将来，随着科技的进步，在“无线着你的无限”，人们的生活方式将发生更大的变革。

4.2 楼宇自动化设计实例

随着计算机技术、控制技术和通信技术的发展，楼宇自动化工业在过去的十年中获得了巨大的发展，遵循 BACnet、LonTalk 和 EIB（European Installation Bus，欧洲设备安装总线协议）这些标准化通信协议的楼控产品在行业中占据着主导地位。使用这些通信协议的楼宇自动化网络所采用的通信传输介质（比如双绞线、同轴电缆和光缆）通常都是有线的，那么无线通信技术有没有可能在楼宇自动化领域占有一席之地并得到广泛应用呢？

和采用有线网络的通信技术楼控产品相比较，无线解决方案最吸引人的地方是安装布置的灵活性、低廉的安装费用和对楼宇自动化系统进行重新布置时的可移动性。尽管无线通信技术和有线相比较有明显的优势，而且蜂窝无线移动通信技术、无线局域网技术和蓝

牙技术已经在市场上获得了巨大的成功，但无线通信技术在楼宇自动化领域应用相对还是很少。这主要是因为目前没有一项无线通信技术适合在楼宇自动化领域进行广泛的推广，而且现有的一些针对楼控领域无线通信产品的价格偏高，导致无线通信技术在楼控领域的应用停滞不前。

4.2.1 楼宇自动化行业动态

随着近年来人类在微电子机械系统（MEMS）、无线通信、数字电子方面取得的巨大成就，使得发展低成本、低功耗、小体积、短通信距离的多功能传感器成为可能。近期所涌现出来的一项新的无线通信技术——ZigBee 技术将改变这种状况。ZigBee 技术产品以其低成本、低功耗、低传输速率、优秀的组网能力，被广泛认为将在未来的几年中对楼宇自动化工业产生重大的影响。

4.2.1.1 无线通信技术在楼宇自动化系统应用的优越性

无线通信技术是利用电磁波在空气中发送和接收数据，而无需线缆介质。在楼宇自动化系统中采用无线通信技术是对系统有线组网方式的一种补充、扩展甚至是替代。无线通信技术使得楼宇自动化设备具有可移动性，它能快速方便地解决使用有线方式所不易实现的网络联通问题。与有线传输方式相比较，在楼宇自动化系统中采用无线通信技术具有低廉的安装费用、灵活性和可移动性等优点，以下是对其的详细阐述：

（1）通常在智能建筑的网络建设中，施工周期最长、对周边环境有影响的往往是综合布线系统，采用无线通信技术最大的优势就是可以免去楼宇自动化系统中网络布线的大部分工作量。

（2）在采用有线传输方式的楼宇自动化网络中，网络设备的安放位置通常受网络信息点位置的限制。但是一旦无线网络建成后，在无线网的信号覆盖区域内任何一个位置都可以接入网络。

（3）由于有线网络缺少灵活性，这就要求楼宇自动化系统的网络规划者尽可能地考虑未来发展的需要，这往往需要预设大量利用率较低的信息点；而一旦网络的发展超出了设计规划，则需要对网络的布局进行重新的考虑，而无线网络可以避免或减少以上情况的发生。

（4）假如对楼宇自动化系统重新进行改造，对于有线网络，消除原有的旧系统和对新系统进行新的布置将带来庞大的工程费用，而无线网络则相反，将会带来巨大收益。

4.2.1.2 无线通信技术目前在楼宇自动化系统应用所面临的问题

尽管在楼宇自动化系统中采用无线通信技术具有有线无可比拟的优势，但目前采用有线传输介质的楼控产品仍然占据着绝对的主导地位，人们在进行楼宇自动化系统设计时，很少会考虑到采用无线通信技术。这主要是因为目前针对楼宇自动化系统的无线产品尚面临着成本、可靠性、适用性和协议的标准化等一系列问题。

另外楼宇自动化系统属于控制网络的一种，控制网络肩负的特殊任务和工作环境，使它具有许多不同于普通计算机网络的特点。控制网络以具有通信能力的传感器、执行器、控制器作为网络节点，并将其连接成开放式、数字化、实现多节点通信，完成监测控制任

务的网络系统。以下是控制网络所需要具备的主要特点：

（1）数据传输量相对较小；

（2）传输效率相对较低，多为短帧传送；

（3）通信传输的实时性强；

（4）抗干扰能力强，可靠性高。

在选择合适的应用于楼宇自动化系统的无线通信技术时，必须对以上的内容进行综合考虑。目前无线通信技术在楼宇自动化领域的应用探讨比较多的主要有无线局域网技术、蓝牙技术和ZigBee技术。无线局域网技术（Wireless Local area network，WLAN）是一种借助无线通信技术取代以往有线布线方式构成局域网的新手段，可提供传统有线局域网的所有功能，它是计算机网络与无线通信技术相结合的产物。蓝牙技术是一种短距离无线连接的无线技术，目的是取代现有的PC、打印机、传真机和移动电话等设备上的有线接口。无线局域网技术和蓝牙技术都不能够完全具备适合在楼宇自动化系统应用的特点。

ZigBee技术是建立在IEEE（Institute of Electricaland Electronics Engineers，美国电气电子工程师学会）802.15.4基础上的无线通信协议，它是一个短距离、低功耗协议，特别适合设计应用在小型的建筑物自动化设备中，比如温度自动调节装置、灯光控制设备、环境传感器等。ZigBee技术能够在低功耗下提供短距离、低速的数据传输，使用普通干电池的ZigBee无线传感器能够持续运行2~3年的时间。另外ZigBee技术优秀的组网能力使得它和其他无线通信技术在楼宇自动化系统中的应用相比尤其具有无可比拟的优势。

4.2.1.3 ZigBee技术分析

ZigBee技术由一个企业之间的团体——ZigBee联盟（ZigBee Alliance）负责制定和推广。ZigBee联盟由霍尼韦尔（Honeywell）、英维思（Invensys）、三菱电气（Mitsubishi Electric）、三星（Samsung）、摩托罗拉、飞利浦（Philips）和Ember七家国际著名公司作为发起方，截止到2009年11月该联盟所参加的企业成员已经超过300家，均为在行业中有重大影响的企业。

ZigBee技术建立在IEEE802.15.4标准技术之上，IEEE802.15.4是一个支持低功耗、低数据传输率的无线网络标准，主要是设计用来进行远程监测与控制的应用。在2003年5月，IEEE802.15.4标准得到了正式批准。IEEE802.15.4是一个简单的但功能却十分强大的数据包协议，它通过确认、错误检测、区分优先次序的通信、DSSS（Direct Sequence Spread Spectrum——直接序列扩频技术，它具有改变频率消除干扰的能力）和用户选择安全等级等技术来提供无线通信的高可靠性。IEEE802.15.4标准同样只规定了开放式系统互联参考模型中的物理层和介质访问子层，其中物理层定义了三个许可的频率波段，它们分别是2.4GHz（最高传输速率250kB/s）、915MHz（最高传输速率40kB/s）和868MHz（最高传输速率20kB/s）。

ZigBee技术在IEEE802.15.4所定义的基础上又增加了网络层、安全层和应用轮廓层（Application Profiles）。ZigBee支持星型、网状和树簇状的网络拓扑结构。在每一个ZigBee网络中最多可以拥有65535个节点，每个节点的地址由ZigBee的网络协调节点（Network Coordinator）负责分配。另外每个节点的传输范围在30~100m之间，而且传输的距离还可以通过使用功率放大器和多跳网状网络结构得到延伸。

ZigBee技术在楼宇自动化领域有广阔的发展和应用前景。首先，ZigBee技术是一项低成本、低功耗的无线解决方案，采用ZigBee技术的无线传感器使用普通的干电池即可工作2~3年的时间，而ZigBee芯片的价格将在1~2年时间内降低到2美元左右；其次，ZigBee技术支持网状网络结构，这使得ZigBee网络具有自组织、自修复的能力，提高了网络的可靠性；第三，ZigBee网络支持数量众多的节点，这点对于大型的楼宇自动化系统中需要大量的传感器和控制器的场合是非常重要的。

4.2.1.4 ZigBee技术在楼宇自动化领域的应用前景

根据美国著名的市场研究机构ABI Research预测：内建ZigBee无线装置的产品将从2005年的100万台发展到2006年的8000万台。ZigBee巨大的发展空间在于其技术上明显的优势以及市场定位的明确。目前国际上楼宇自控方面专家基本上达成了共识，无线通信技术在楼宇自动化的应用将不可阻挡。无线网络将不仅仅是对有线网络有益的补充、扩充，而可能是替代作用。

在使用ZigBee技术的楼宇自动化系统中，无线网络的框架是网状结构，使用一定数量的ZigBee路由器节点即可覆盖整个的建筑内部区域，而且节点数越多，系统将越可靠。另外由于网状网络结构具有自配置的功能，增加新的节点时或重新对节点进行布置时将十分方便。而无线网络的边缘是星型结构，大量内建ZigBee无线装置的传感器或者执行器被接入网络，这些传感器使用普通的干电池就可以工作2~3年时间。

ZigBee技术的融入比较简单的做法是在ZigBee网络和这些异种网络之间建立相关网关作为它们之间的桥梁，那么ZigBee将是这些有线网络的有益补充，届时整个楼宇自动化系统将出现无线网络和有线网络共存的局面，从而获得较高的经济效益。更为完善的做法是在ZigBee技术的基础上建立与BACnet、LonTalk通信协议相类似的适用于楼宇自动化领域的整套无线通信协议，这种情况下ZigBee将能够和这些通信协议并驾齐驱，并有可能最终替代这些主要采用有线网络的通信协议。

随着我国经济的迅速发展，智能建筑的数量将会越来越多，选择适合我国国情的楼宇自动化技术及产品是人们迫切需要关注的一个问题，但目前我国智能建筑中所使用的楼控系统及产品大多被国外的大公司所垄断，ZigBee技术的出现将给我国开发自主的具有世界先进水平的楼宇自动化系统及产品提供一个崭新的契机。

LonWorks控制网络技术以其开放性、低成本、开发迅速的特点在楼宇自动化方面得到了广泛的应用，但是它同时也具有有线网络的布线复杂、灵活性和可扩展性不好等缺点。ZigBee技术是一种近距离、低复杂度、低功耗、低数据传输率、低成本的双向无线通信技术，符合IEEE802.15.4标准，是IEEE工作组专门为短距离通信制定的新标准。

ZigBee技术融入比较简单的办法就是在ZigBee网络和这些异构网络之间建立网关作为它们之间的桥梁。在楼宇自动化系统中实现无线网络和有线网络共存的局面，从而获得较高的经济效益。本节就设计了这样一个基于LonWorks控制网络和ZigBee无线网络相结合的楼宇智能化网络系统。

4.2.2 系统设计

系统的体系结构如图4-4所示。众多ZigBee节点设置在智能楼宇的中央空调子系统、

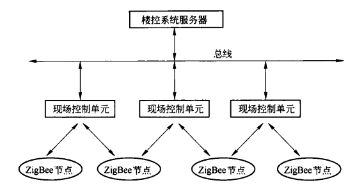


图 4-4　楼宇智能化网络系统体系

冷量计费子系统、锅炉/热交换子系统、给排水子系统、变配电子系统、照明灯光子系统、电梯子系统、防盗保安子系统中，实时监测和控制各个子系统，同时实时将各子系统监控的状态变化以无线方式传送给位于各个检控点附近的现场监控单元。现场监控单元既是智能节点，同时也是 ZigBee 的网关节点。

每个系统可根据实际情况划分若干个监控区域，每个监控区域设置一个现场监控单元和若干 ZigBee 智能节点。现场监控单元对 ZigBee 节点传来的采集数据进行处理后，通过总线将数据发送到系统服务器。位于楼宇控制室的中央处理服务器，是楼宇监控系统的主处理服务器，是系统逻辑处理核心。中央处理服务器从分布在监控区域的现场监控单元和实时状态数据，对接收到的数据进行逻辑处理和分析，如存储归档、阈值比较、阈值调优和趋势分析等，并根据分析的结果通过用户工作站向用户发布事件、警告和预警信息。还可根据需要下达控制指令，对 ZigBee 节点进行控制。

现场监控单元是系统的主要组成部分，负责各个子系统现场实时状态数据的收集、缓存和转发，并根据来自中央处理服务器的指令进行相应的通信处理和控制，如图 4-5 所示。由于现场监控单元主要安装在各个系统的终端区域，容易受各种噪声和电磁干扰，其

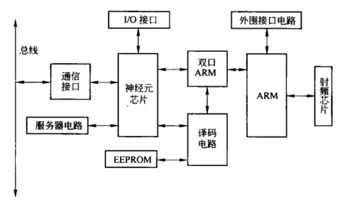


图 4-5　现场监控单元

可靠性、可用性、可维护性、安全性和实时性等构成整个系统关键，因此现场监控单元是整个系统设计重点和关键所在。

这是一种基于 Host-Based 结构的 LonWorks 智能节点，主要包括 ARM 处理器、ROM、RAM、神经元处理、无线射频芯片等。其中 ARM 主要进行复杂的数据处理及控制功能，这样就可以解决 Neuron 芯片内部资源紧张的问题，神经元芯片主要完成通信功能，它能够将主处理器经过处理传过来的数据通过收发器发送到 LON 总线，也可以将 LON 总线上的消息接收至本节点。

ZigBee 节点采用电池供电，节点体积受安装环境制约，要尽可能小，而且有效工作时间也要尽可能长，无线通信需要电池提供足够大的电流，耗电量比较大，所以低功耗设计成为节点设计的重点和难点。节点采用低功耗 ZigBee 芯片 CC2430，如图 4-6 所示。

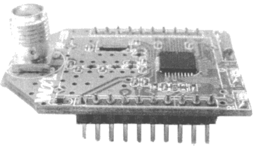


图 4-6 ZigBee 节点

4.2.3 网络结构设计

网络结构设计是提供楼宇自动化系统中位于各个子系统中的所有设备的互联互通方案，如图 4-7 所示，以实现：中央处理服务器从现场监控单元获取监测信息；用户工作站

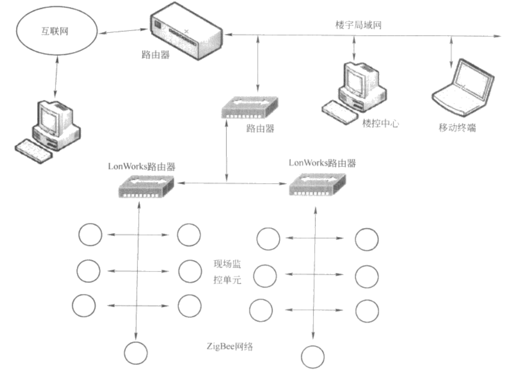


图 4-7 网络结构

从中央处理服务器获取监测信息；网管工作站监视楼宇自动化系统通信网络上网络设备。

楼宇自动化系统网络包括控制室内的以太局域网及现场监控单元与车站中央处理服务器 CPS 组成的现场控制总线网络以及终端的 ZigBee 无线网络三部分，相应地，通信骨干也划分为三部分，其通信时序如图 4-8 所示。

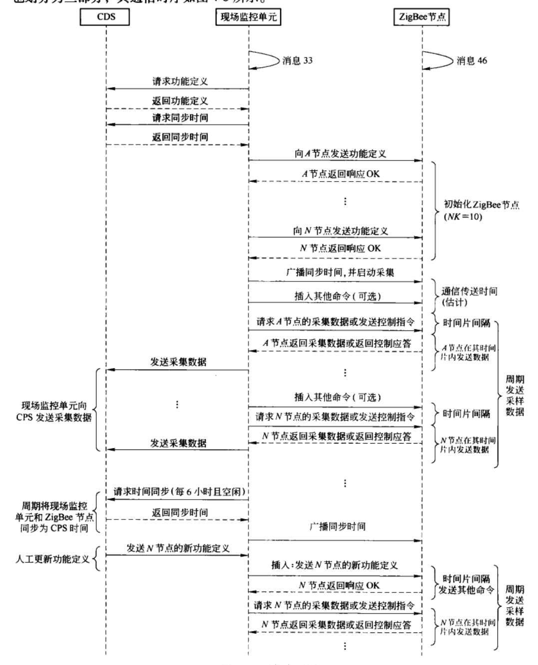


图 4-8 通信序列图

（1）以太局域网。楼宇控制室内的以太局域网组网比较简单，介质采用5类双绞线，通信协议采TCP/IP协议。

（2）现场控制总线网络。由于监控区域遍布整个楼宇，比较分散，所以在系统设计中选定采用现场控制总线Lon-Works技术（可以自由拓扑组网）作为现场监控单元与控制室内中央处理服务器之间的通信网络平台。

现场控制总线网络由1个光纤或双绞线干线及多个总线形双绞线分支组成。每个双绞线总线分支上挂接一组地理位置相对集中的现场监控单元，每个双绞线总线分支通过Lon-Works路由器挂接在光纤或双绞线干线上。如果干线采用光纤，则LonWorks路由器可以放置在控制室外接近监测区域的地方，如果采用双绞线，由于总线长度限制（1.25M速率下120m距离），LonWorks路由器只能放置在总控制室内或每楼层的设备室内。

当LonWorks路由器放置在控制室外距现场监控单元较近处时，若本组总线长度不超过120m，总线速率可达1.25M，否则只能采用78k速率（2km）。

（3）ZigBee无线网。ZigBee节点采用IEEE802.15.4/ZigBee协议与现场监控单元通信。

4.2.4 软件总体框架

软件总体框架图如图4-9所示。系统由人机界面（Man Machine Interface，MMI）、中

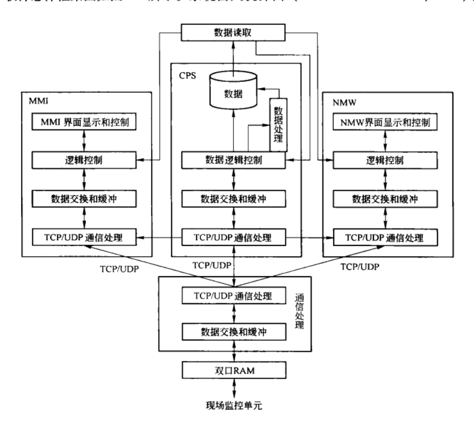


图4-9 软件总体框架图

央处理服务器（Centre Process Server，CPS）、网管工作站（Network Monitoring Workstation，NMW）及通信处理4个模块组成。

楼宇控制室的中央处理服务器既是楼宇自动化系统的主处理服务器，也是系统逻辑处理核心。中央处理服务器对接收到的数据进行逻辑处理和分析，如存储归档、阈值比较、阈值调优和趋势分析等，并根据分析的结果通过用户工作站向用户发布事件、警告和预警信息。

同时，中央处理服务器根据监测数据信息，向相应现场监控单元发送控制指令，然后该现场监控单元经过指令分析和ID确认后通过无线网向相应的ZigBee节点发送控制指令。另外，中央处理服务器接收并处理用户通过用户工作站发出的“点播”、“开启”、“关闭”某个监测对象的实对监测采样等指令，并向相应的现场监控单元转发指令。

通信处理模块从LonWorks总线上获取现场采集数据并将相应数据发送到MMI、CPS、NMW，同时将来自MMI、CPS、NMW“点播”等指令下达到相应的现场监控单元。完成数据通信与数据处理之间的数据交换，并为输入和输出的数据提供内部缓冲。

用户工作站位于总控制室，运行在其上的MMI软件直接面向操作员，所有从现场实时监测到的数据及中央处理服务器分析判断的结果均通过MMI向用户呈现，MMI是楼宇自动化系统最重要的部分之一。

为了足够的用户友好，MMI提供一个整个楼宇自动化系统的视图，在该视图上，无监测区域是简化显示，监测区域为重点显示对象，另外，还可以看到监测区域对应的现场监控单元。正常情况下，监测区域为绿色显示。如果监测到故障（现场监控单元故障或监测值超过阈值），现场监控单元将用红色闪烁显示并伴随声光报警。如果监测值趋势分析产生预警时，现场监控单元将用黄色闪烁显示。

用户可通过MMI“点播”某个现场监控单元的某个监控对象（ZigBee节点）的实时动态变化曲线，也可以通过MMI启动或关闭某个现场监控单元对某个监控对象（ZigBee节点）的监测。为了帮助用户及时定位和排除局域网和现场控制网络的故障，网管工作站NMW同时与局域网和现场控制网络相连，运行在网管工作站NMW上的网管软件可以集中监视两个网络的状态。

ZigBee传感器和现场中心收集设备（SimpleSensor和SimpleCollector）。中心收集设备作为协调器或路由器启动。中心设备描述符为：

```
const SimpleDescriptionFormat_t zb_SimpleDesc =
{
  MY_ENDPOINT_ID,                    // 端点
  MY_PROFILE_ID,                     // Profile ID
  DEV_ID_COLLECTOR,                  // 设备 ID
  DEVICE_VERSION_COLLECTOR,          // 设备版本
  0,                                 // 保留
  NUM_IN_CMD_COLLECTOR,              // 输入命令数量
  (cId_t*)zb_InCmdList,              // 输入命令列表
  NUM_OUT_CMD_COLLECTOR,             // 输出命令数量
  (cId_t*)NULL                       // 输出命令列表
```

```
};
```

传感器设备作为终端设备启动。传感器设备的描述符为：

```
const SimpleDescriptionFormat_t zb_SimpleDesc =
{
  MY_ENDPOINT_ID,                        //  端点
  MY_PROFILE_ID,                         //  Profile ID
  DEV_ID_SENSOR,                         //  设备 ID
  DEVICE_VERSION_SENSOR,                 //  设备版本
  0,                                     //  保留
  NUM_IN_CMD_SENSOR,                     //  输入命令数量
  (cId_t *)NULL,                         //  输入命令列表
  NUM_OUT_CMD_SENSOR,                    //  输出命令数量
  (cId_t *)zb_OutCmdList                 //  输出命令列表
};
```

绑定建立成功之后，传感器设备将根据定义的时间间隔周期的采集温度传感器和电池电压值，分别通过报告命令发送给收集设备。该报告命令要求收集设备应答，通过函数zb_SendDataConfirm可以指示应答，如果传感器设备有一个应答没有接收到，传感器设备将移除它存在的绑定，然后进行重新发现和绑定过程。

通过函数 zb_HandleOsalEvent 完成用户定义的事件，程序清单如下所示：

```
//*****************************************************************
//函数原型:void zb_HandleOsalEvent( uint16 event)
//输入：事件
//输出：无
//功能描述：用户定义事件处理函数
//*****************************************************************
void zb_HandleOsalEvent( uint16 event)
{
  uint8 pData [2];
  if( event & MY_START_EVT)
   {
    zb_StartRequest( );
   }
  if( event & MY_REPORT_TEMP_EVT)              //  温度报告
   {
    //读温度值
    pData[0] = TEMP_REPORT;
    pData[1] =   myApp_ReadTemperature( );
    zb_SendDataRequest(0xFFFE,SENSOR_REPORT_CMD_ID,2,pData,0,AF_ACK_REQUEST,0);
    osal_start_timer( MY_REPORT_TEMP_EVT,myTempReportPeriod);
   }
  if( event & MY_REPORT_BATT_EVT)              //  电池报告
```

```
    {
    //读电压值
    pData[0] = BATTERY_REPORT;
    pData[1] =   myApp_ReadBattery();
    zb_SendDataRequest(0xFFFE,SENSOR_REPORT_CMD_ID,2,pData,0,AF_ACK_REQUEST,0);
    osal_start_timer(MY_REPORT_BATT_EVT,myBatteryCheckPeriod);
   }
}
```

收集节点接收到传感器设备发送的数据包后，它能显示到PC机或LCD上。采用串口传输到PC机，通过串口调试工具可以观察到。该过程通过接收数据指示函数zb_ReceiveDataIndication完成，程序清单如下所示：

```
//*****************************************************************
//函数原型:void zb_ReceiveDataIndication(uint16 source,uint16 command,uint16 len,uint8 * pData)
//输入：源地址，命令，数据长度，数据
//输出：无
//功能描述：接收数据指示
//*****************************************************************
//静态常量定义
CONST uint8 strDevice [] = " Device: 0x";
CONST uint8 strTemp [] = " Temp: ";
CONST uint8 strBattery [] = " Battery: ";
void zb_ ReceiveDataIndication (uint16 source, uint16 command, uint16 len, uint8 * pData  )
{
  uint8 buf [32];
  uint8 * pBuf;
  uint8 tmpLen;
  uint8 sensorReading;
  if(command == SENSOR_REPORT_CMD_ID)  //保证命令正确
   {
    //读取传感器数据
    sensorReading = pData [1];
    //写信息到串口
    tmpLen = (uint8)osal_strlen((char * )strDevice);
    pBuf = osal_memcpy(buf,strDevice,tmpLen);
    _ltoa(source,pBuf,16);
    pBuf + =4;
    * pBuf ++ =' ';
    if(pData[0] == BATTERY_REPORT)  //电池电压
     {
      tmpLen = (uint8)osal_strlen((char * )strBattery);
      pBuf = osal_memcpy(pBuf,strBattery,tmpLen);
      * pBuf ++ = (sensorReading/10) +'0';      //转换 MSB 为 ascii
```

```
            *pBuf++ ='.';                              //小数点
            *pBuf++ = (sensorReading % 10) +'0';       //转换 LSB 为 ascii
            *pBuf++ =' ';
            *pBuf++ ='V';
        }
        Else // 温度
        {
          tmpLen = (uint8)osal_strlen((char *)strTemp);
          pBuf = osal_memcpy(pBuf,strTemp,tmpLen);
            *pBuf++ = (sensorReading/10) +'0';      //转换 MSB 为 ascii
            *pBuf++ = (sensorReading % 10) +'0';     //转换 LSB 为 ascii
            *pBuf++ =' ';
            *pBuf++ ='C';
        }
        *pBuf++ ='\r';
        *pBuf++ ='\n';
        *pBuf ='\0';
#if defined(MT_TASK)
        debug_str((uint8 *)buf);
#endif
        //为了方便，这样也可以调用串口驱动函数，直接把接收到的数据写到串口
    }
}
```

本节对基于 ZigBee 技术和 LonWorks 总线技术相结合的智能楼宇自动化系统进行了探讨。经测试表明，该系统结合了两种技术的优点，具有良好的实用性能。我国经济发展迅速，智能建筑的数量将会越来越多，选择适合我国国情的楼宇自动化产品是人们迫切需要关注的一个问题。随着 ZigBee 技术的不断发展，其低成本、低功耗、较远的覆盖距离等特点成为楼宇自动化系统新的亮点，这也将给我国开发自主的具有世界先进水平的楼宇自动化产品提供一个崭新的契机。

4.3 医疗保健设计实例

现在，在许多人们最关心的日常事务中，对健康的关心排在了靠前的位置。对健康的关心程度可通过昂贵的保险费用、降低的生产力甚至雇员的调整直接影响到公司的盈亏。然而，对健康关心，与比财务问题相比是个更深层次、更个人化的问题。2/3 超过 65 岁的人需要长期护理，所需长期护理的平均时间超过 3 年，而绝大多数人在某些程度上都有可能受此影响。因此，随着人均寿命的持续提高，高质量的长期护理就成为了全世界关注的焦点。

4.3.1 应用需求

通过在病人家中的远程协助，自动监护系统可帮助增加病人的安全性，改善生活质量。很不幸的是，现在大多数监护系统仍然要限制病人的自由行动。然而，新近的无线技

术使得病人摆脱了医疗器械的束缚，自由行动成为了可能，同时又为护理者提供了更高效的建立护理网络的方法。这也使得健康工作者在这个过程中监护病人们成为了可能。

长期护理包含了多种改善或维持病人生活质量而设计的服务。当有许多条件可要求长期护理时，高龄是寻求长期护理的第一条件。1949 年，我国的人均寿命是 35 岁。到 2009 年，这一数字已增加到了 73 岁。20 世纪 50 年代上半期，世界人口预期寿命为 46.5 岁，其中经济发达国家的人口预期寿命为 66.1 岁，发展中国家的人口预期寿命为 41 岁；20 世纪 90 年代下半期，世界人口预期寿命为 65 岁，其中经济发达国家的人口预期寿命为 74.9 岁，发展中国家的人口预期寿命为 63 岁。2004 年底，我国 60 岁及以上老年人口为 1.43 亿，2014 年将达到 2 亿，2026 年将达到 3 亿，2037 年超过 4 亿，2051 年达到最大值，之后一直维持在 3 亿 ~4 亿的规模。

我们如何在优化病人护士比率的同时增加病人长期护理的安全性、改善其生活质量？对这个问题的关注在病人、家属、护理提供者及商业公司中持续增长。2000 年，光在美国救济所就有平均 1400000 的患者。这些患者的护理要求大相径庭，18% 抱怨护士常驻家中，而 10% 的患者则生了压迫性溃疡（褥疮）。

4.3.2 技术发展

ZigBee 联盟 2009 年 6 月宣布康体佳健康联盟（Continua Health Alliance）已认可 ZigBee Health Care（医疗保健标准）成为康体佳低功耗局域网（LAN）的新标准。ZigBee Health Care 提供了不受干扰的无线连接，可在单一网络上支持数千部设备。康体佳健康联盟推荐选择 ZigBee 用于专业环境、家庭、活动中心、大型校园内的传感与控制。康体佳健康联盟是由业界各大医疗保健公司与科技公司所组成的重要的非营利联盟。

纳入康体佳健康联盟设计指南的 ZigBee Health Care，提供安全、稳固、电池高效的无线连接，不但能监测病患活动与设施，同时还能在建筑物以外的地方提供无线操作。ZigBee 能与 Wi-Fi 等其他无线技术和平共存，这是保护医疗设施内病患安全及确保应用时不可或缺的关键要求。ZigBee Health Care 可以在世界各大半导体制造商具成本效益且已认证的各类硅平台上执行。

康体佳健康联盟总裁兼董事会主席 Rick Cnossen 表示："康体佳健康联盟之所以选择 ZigBee Health Care，是因为在严谨的技术审查之后，第一手发现 ZigBee Health Care 确实有能力符合康体佳健康联盟规定的要求。ZigBee Health Care 可运用于世界各地不同环境，特别适合用于低功耗的 LAN 应用。"

采用该标准的产品可协助老年人与残疾人维持独立的生活，此外这类产品还具备了保护个人数据及符合法律规定时所需要的安全性。

皇家飞利浦电子公司高级主管兼康体佳健康联盟董事会成员 Paul Coebergh van den Braak 表示："作为医疗保健业著名公司之一的飞利浦，在多种产品中都运用了 ZigBee Health Care。ZigBee Health Care 这项全面标准可应用于个人监测，还可搭配医疗设施使用。"

ZigBee Health Care 设备可以与消费电子、家庭自动化、商业建筑自动化中已部署的其他 ZigBee 无线技术交互。

ZigBee 联盟主席 Robert F. Heile 博士表示："ZigBee 联盟期待与康体佳健康联盟维持长

期且有成效的关系，此外并感谢他们将 ZigBee Health Care 纳人康体佳健康联盟设计指南。ZigBee Health Care 现在已经可以让产品制造商使用，而且背后还有一群强大的供货商支持，他们所提供的认证平台可符合任何设备需求。”

大体上，ZigBee Health Care 是互操作无线设备的全球开放标准，可安全监测及管理慢性疾病、肥胖、老化这类非重大、低危险病症的保健服务。ZigBee Health Care 完整支持 IEEE11073 设备。该标准设计用于家庭、健身中心、退休小区、养老院及各种医疗设施，并符合消费者、服务提供者、医护人员、付款人、产品制造商及政策制订者的要求。ZigBee Health Care 认证产品可以与住宅和商业环境中的其他 ZigBee 认证产品交互。

4.3.3 技术方案

因为长期护理是 21 世纪的问题，所以我们用 21 世纪的方案去解决。对于医疗护理者来说，快速、准确访问患者信息能提高护理质量。医疗对策不仅仅局限于患者床边，护理质量往往取决于护理器械之外的与临床医生实时共享病人生理数据的能力。这意味着临床医生可以基于实时临床实验研究结果，立即给主治医师提供反馈，同时还能跟踪在医院之外的治疗途径和效果，从而改进以后的治疗方法。

ZigBee 技术被很快证明能有效应用在这些应用中，用于帮助患者摆脱自动监控设备的束缚，获得更大的自由行动能力。通过提供低成本、低功耗的无线技术，利用网状网络，它就能覆盖大厦和公共机构。ZigBee 技术可以配置到许多产品中，以帮助确保对患者更好的护理和更有效的护理跟踪。

长期护理患者所需的远程自动监控系统可分为多种，包括：（1）患者监控；（2）行动监控；（3）安全监控；（4）事件捕捉。

患者监控系统通常检查生命迹象，如心跳速率和体温，或者疾病征兆如血压和血糖等级。ZigBee 可以用来传输数据到网关，当这些数据中的某个值超出极限时提醒监控人员。自动监控系统甚至可以设计为执行特殊命令。举个例子：监控血糖等级，根据预设间隔值记录血糖数据。如果血糖等级超出极限值，就自动注射胰岛素。

行动监控系统监控每天的行动。记录的数据可用来分析变化。从每天的运动或锻炼中，用加速度传感器跟踪运动数据是非常简单的。这些数据可与从患者身上采集的信息（如心跳速率）作比较，以确定一定量的锻炼对身体有多少作用。人体行动可以被跟踪任意长时间，然后与历史数据相比，以鉴别某种倾向。甚至可以利用行动监测系统来提醒患者做运动，或者提醒护理人员患者是否做了运动。

安全监测系统以事件提醒或潜在的可能影响患者安全的事件提醒为目标，如当患者离开监测区域时，监护者会收到提醒，并重新定位患者所在区域。

事件捕捉系统记录患者相关事件和监护者响应情况。这是重要的健康护理信息，并能保证事件信息和相应行动能被快速找回并检查。

4.3.4 节点设计

飞思卡尔家族的 ZigBee 技术为医疗监护应用的需求提供了完美的低成本、低功耗、高集成度和高性能的解决方案。这些解决方案中包括了系统级 32 位嵌入式控制器和平台级封装（PiP）的 32 位 MC13224 解决方案，如图 4-10 所示。

飞思卡尔的第三代 MC13224 是运用 ZigBee 技术的医疗应用的理想平台。它能为减小产品尺寸和降低产品成本提供关键技术改进，这对于穿戴在身上的设备来说尤为重要。高度集成的低功耗设计使电池的续航能力大大增加，而且只需要一个外接电源和一个 50Ω 的天线即可完成此方案。32 位 ARM7 核心处理器拥有充足的储存空间，能在单个 IC 上运行 ZigBee 协议栈和用户应用程序。

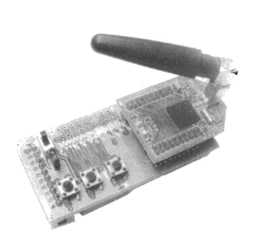


图 4-10　ZigBee 节点

ZigBee 解决方案不只包含了芯片本身，而且还包括了软件、开发工具和参考设计来帮助简化开发。MC13224 的 ZigBee 适用的 BeeStack 和 BeeKit 无线工具包提供了配置网络参数的简单软件环境。这个工具使得用户可以用向导和下拉菜单来帮助它们配置 ZigBee 网络参数，而竞争对手的解决方案却使用户不得不通过改动代码来配置网络参数。

同时，像 MC13224 这样的 PiP 解决方案简化了射频设计，用户则可不必有专门的经验来保证设计的鲁棒性和最优性。所以 MC13224 已经为客户在这方面做了许多工作，搜集了许多参考设计，用户可以拿到它们的 BOM、印刷电路板文件和原理图，并可以通过简单拷贝参考设计来集成到用户自己的产品中。提供一个完整的平台方案可以帮助用户缩短产品开发时间并快速占领市场。

老年人和长期医疗护理将持续成为我们社会的重要问题。先进的技术能针对需求改善患者的生活质量，而 ZigBee 无线技术能带给设计者们新的设计理念。低功耗的无线解决方案可用于患者行动监护和安全监护，ZigBee 技术为患者提供了他们所要的更高自由度，同时也提供给监护人员许多重要优势，包括：

（1）高性价比和可升级的网络以应对紧急响应处理情况下的瓶颈。

（2）实时提示不符合常规医疗惯例的输液方案，从而消除可预防的不良医疗事故。

（3）有机会改进治疗草案。

（4）医生可在他们的办公室内远程访问患者实时数据。

（5）实时分析药物疗效。

（6）实现所有相互连接的医疗器械的网络化管理。

（7）实时患者治疗能降低成本，改进护理。

通过我们先进的 ZigBee 技术解决方案，本系统使用户能设计出新的产品以帮助用户快速占领医疗器械市场，并改善需要长期护理的患者的日常生活。

4.3.5　代码分析

建立 ZigBee 无线网络：

```
/*********************************************************************
NetworStartSucc
```

```
网络建立成功,网络状态切换,显示监控状态
*********************************************************************/
void NetworStartSucc(void)
{
    NetState = mStateZDO_device_running_c;//网络状态切换
    ClearScreen();
    Print(0,25,"网络协调器",1);
    Rectangle_x(0,4,127,7);
    Print(2,13,"网络监控中...",1);
    Print(5,5," >                ",1);
    Runflag = 1;
    TMR_StartSingleShotTimer(RunTimerId,RunReportTime_c,RunTimerCallBack);//启动超时定时器
}
```

主函数如下:

```
#ifdef __IAR_SYSTEMS_ICC__
  void Main(void)   {
/* First init the Interrupt module */
  InterruptInit ();
  /* Interrupts should already be off. This is probably redundant. */
  IntDisableAll ();
  /* Set priority and handler for Crm, timer, and maca */
  /* Init the radio and set the channel */
  Platform_Init();
  TS_Init();
  TMR_Init();
  Uart_ModuleInit();
  /* initialize all tasks */
  BeeStackInit ();
  /* initialize MAC after stack */
  Init_802_15_4(TRUE);
  /* NvModuleInit (); is already called in the function above BeeStackInit (); this comment fix ticket 433 */
  LED_Init();
  /* initialize the application */
  gAppTaskID = TS_CreateTask(gTsAppTaskPriority_c,BeeAppTask);
  BeeAppInit ();
  /* All LED's are switched OFF */
  Led1Off ();
  Led2Off ();
  Led3Off ();
  Led4Off ();
  Led1On ();
  IntEnableAll ();
```

```
#else/ * __IAR_SYSTEMS_ICC__ * /
  void main (void) {
  / * Interrupts should already be off. This is probably redundant. * /
  IrqControlLib_DisableAllIrqs();
  Init_802_15_4();
#if gBeeStackIncluded_d
  TS_Init();                                    / * Init the kernel. * /
  Uart_ModuleInit();
  BeeStackInit();
#else
  TMR_Init();
#endif
  gAppTaskID = TS_CreateTask(gTsAppTaskPriority_c, BeeAppTask);
  BeeAppInit ();
  IrqControlLib_EnableAllIrqs();
#endif  / * __IAR_SYSTEMS_ICC__ * /
  / * Start the task scheduler. Does not return. * /
  TS_Scheduler();
}
```

节点加入 ZigBee 无线网络：

```
uint8_t        NetState = mStateIdle_c;    //网络状态
/ ***********************************************************************
NetworJionSucc                         成功加入网络。
***********************************************************************/
void NetworJionSucc (void)
{
    uint8_t   * pNwkAddress;
    uint16 Saddr;
    uint16 temp;
    NetState = mStateZDO_device_running_c;
}

enum {
    mStateIdle_c,
    mStateZDO_init_device_c,
    mStateZDO_Coordinator_starting_c,
    mStateZDO_stopped_c,
    mStateZDO_network_discovery_c,
    mStateZDO_join_network_c,
    mStateZDO_device_running_c,
    mStateZDO_device_unauth_c,
    mStateZDO_orphan_c,
```

```
    mStateMatchDescRequest_c,
    mStateMatchDescSuccess_c,
    mStateBindRequest_c,
    mStateBindSuccess_c,
    mStateUnBindRequest_c,
};
```

定时采集传感器数据函数:

```
/************************************************************************
  ContinuumTxTimerCallBack 定时器事件触发
************************************************************************/
char sysLED2Value = 0;
char Startflag = 1;
void ContinuumTxTimerCallBack  (tmrTimerID_t timerId)
{
    uint16 temp1;
    uint8_t   * pNwkAddress;
    (void)timerId;  /* to prevent compiler warnings */
    if(Startflag)//首次进入定时器函数
    {
        Startflag = 0;
        TMR_StopTimer(ContinuumTxTimerId);
    }
    else
    {           //LED 闪烁
            if(sysLED2Value == 0){
                    sysLED2Value = 1;
                    Led2On();
                }
            else{
                    sysLED2Value = 0;
                    Led2Off();
            }
    TMR_StartSingleShotTimer(ContinuumTxTimerId, ContinuumTxReportTime_c, ContinuumTxTimerCall-
Back);//启动超时定时器
    memset(RfTx.TxBuf,'x',29);
    RfTx.TXDATA.HeadCom[0] = 'T';
    RfTx.TXDATA.HeadCom[1] = 'W';
    RfTx.TXDATA.HeadCom[2] = 'D';
    memcpy(RfTx.TXDATA.Laddr,gNwkData.aExtendedAddress,8);
    pNwkAddress = APS_GetNwkAddress(RfTx.TXDATA.Laddr);
    RfTx.TXDATA.Saddr[0] = *pNwkAddress;
    RfTx.TXDATA.Saddr[1] = *(++pNwkAddress);
```

```
        templ = ReadAdc1(mAdcChannelPhoto_c);          //光敏
        sprintf((char * )&RfTx.TXDATA.DataBuf[0],"light: %d",templ);
    TS_SendEvent(gAppTaskID,gDataSend);//发送数据
    RfSendData(0x0000,RfTx.TxBuf,31);//发送自己的节点信息到主机
    }
}
```

4.4 无线抄表设计实例

随着现代科技的飞速发展，无线抄表系统越来越受到人们的青睐并逐渐取代了传统的抄表系统。传统抄表系统大致可以分为三类，即智能卡水表、有线自动抄表系统、无线智能水表。其中有线自动抄表系统又可分为分线制集中抄表和总线制集中抄表。由于前两种方式都存在着不利因素，故目前无线自动抄表系统越来越受到业界的瞩目。

4.4.1 应用需求

长期以来，三表数据抄送问题都是相关供应部门非常想解决但又得不到切实解决的问题。在行业信息化过程之中，户表数据的自动化抄送具有非常重大的意义，因为户表数据是相关行业销售过程中最原始的数据，这个数据的准确度和及时性直接影响了行业内部其他信息化水平。

传统的手工抄表费时、费力，准确性和及时性得不到可靠的保障，这导致了相关营销和企业管理类软件不能获得足够详细和准确的原始数据；一般人工抄表都按月抄表，对于用户计量来说是可行的，但对于相关供应部门进行更深层次的分析和管理决策却不够，行业的实际需求催生着自动抄表系统的技术和应用的不断发展。

随着无线通信技术的不断发展，近年来出现了面向低成本设备无线联网要求的技术，称之为 ZigBee，它是一种近距离、低复杂度、低功耗、低数据速率、低成本的双向无线通信技术，主要适合于自动控制、远程控制领域及家用设备联网，我们采用 ZigBee 技术和 GPRS/CDMA 技术结合，可以为水表的无线抄表提供很好的解决方案。

4.4.2 技术要求

无线抄表系统对无线通信数据的传输和保存有着很高的要求，即数据可靠性要求很高；由于用电池供电，因此对功耗要求也很苛刻；无线抄表系统可以摆脱人工抄表的办法，利用数据通信协议传输数据；基于以上原因，要求设计的自动无线远传抄表系统应该具有计量准确、通信可靠、抄表方便、功耗低等远程抄表系统的优点，以及节省人力、远程监控、远程维护的功能。

同样是无线抄表系统，相对于电表而言，水表的抄表系统存在更多的技术难题，这主要体现在抄表终端的设计上。归纳起来，水表的抄表终端必须解决以下几个方面的技术要求：

（1）供电。由于水表的抄表终端采用电池供电，因此，对功耗要求非常苛刻。一般而言，电池的使用时间至少要在 3 ~ 6 年，这取决于电池的容量、设备的耗电情况、设备的运行要求等因素。

（2）防水。水表所处的特殊环境总是与水、潮湿分不开的，因此抄表终端必须在防潮、防水方面仔细考虑，要能够在这样的环境下长时间正常工作。

（3）成本。无论是家庭用户，还是企业用户，抄表终端的成本始终是绕不开的话题，特别是家庭用户，对于成本更为敏感。这里的成本包括两个部分：一是，一次性改造或者安装的成本；二是，系统的运行成本。最好的方案应当是一次性投入的成本尽可能低，运行成本没有或者非常低。

（4）对水表故障检测。人工抄表除了抄读水表读数外，同时还担负着检查水表工作是否正常的任务。如果改为自动抄表系统，那么该系统应当也具备对水表故障的自动检测功能。当然，这需要水表与抄表终端的配合才能实现。

（5）通信可靠性。这是无线抄表系统最基本的要求，但同时又是不很容易解决的问题。

（6）无线网络的自组织、自愈功能。

1）自组织功能：无需人工干预，网络节点能够感知其他节点的存在，并确定连接关系，组成结构化的网络。

2）自愈功能：增加或者删除一个节点，节点位置发生变动，节点发生故障等，网络都能够自我修复，并对网络拓扑结构进行相应的调整，无需人工干预，保证整个系统仍然能正常工作。

具备自组织、自愈能力的自动抄表网络才是最理想的网络，ZigBee 技术能够很好地支持这种智能型的网络。

4.4.2.1 ZigBee 技术特点

（1）通信可靠。系统采用了 CSMA-CA 的碰撞避免机制，避免了发送数据时的竞争和冲突；采用完全确认的数据传输机制，保证信息传输的可靠性。

（2）网络的自组织、自愈能力强。

1）ZigBee 自组织功能：无需人工干预，网络节点能感知其他节点的存在，并确定连接关系，组成结构化的网络。

2）ZigBee 自愈功能：增加、删除或移动节点，节点发生故障等，网络都能够自我修复，无需人工干预，保证整个系统仍然能正常工作。

（3）成本低廉。设备的复杂程度低，且 ZigBee 协议是免专利费，这些可以有效地降低设备成本；ZigBee 的工作频段灵活，为免执照频段的 2.4GHz，就是没有使用费的无线通信。

（4）网络容量大。一个 ZigBee 网络可以容纳最多 254 个从设备和一个主设备，一个区域内可以同时存在 200 多个 ZigBee 网络。通过前面对自来水抄表系统的技术要求分析，结合 ZigBee 技术特点和技术优势，采用 ZigBee 技术来实现水表的无线抄表是一个非常理想的解决方案，如图 4-11 所示。

在实际应用中，我们选择了将 ZigBee 技术与 GPRS/CDMA 结合起来，根据抄表用户的不同分布，来灵活地构建抄表的无线网络。

对于每个抄表终端而言，要求超低功耗、低成本（包括设备成本、运行成本），并且数据的传输速率不高，对于居民小区的抄表，抄表终端通常分布较密集、距离较近，

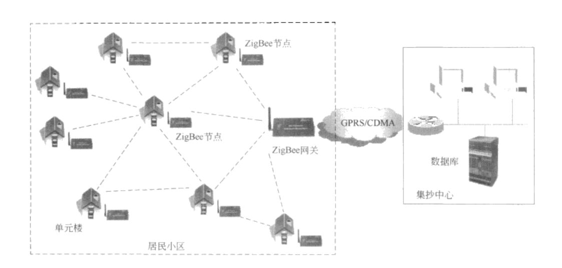


图4-11 系统框图

ZigBee技术可以很好地满足这些要求；终端采集的数据需要送到自来水公司集抄管理中心，这可以通过GPRS/CDMA网络来实现，它无距离限制，且无需网络规划、几乎不需要维护；所构建的ZigBee网络既可以是星型拓扑，也可以是网状网络拓扑，不论是哪种拓扑结构的ZigBee网络，应根据实际的组网需要，设计合理的网络结构。

4.4.2.2 ZigBee技术方案优势

目前的自动抄表系统，从数据传输角度划分，可分为有线、无线两大类。这两大类抄表系统各有其适用的应用领域，但就抄表系统的投资、建设、维护等几方面而言，无线抄表系统显然具有更大优势。

目前市场上的无线抄表系统大致可分为基于无线数传模块、基于GPRS/CDMA数字蜂窝网络或者是两者结合等几种方式，从应用角度而言，都存在以下一种或几种问题：

（1）GPRS/CDMA数据传输需要付费，对于家庭水表抄表来说，系统的运行成本很高。

（2）采用无线数传模块，除了数据轮询时间随节点数增加而线形增加外，所组建的无线网络的自管理功能非常有限，增加或者减少节点，都需要人工去修改相应的数据库配置；节点出现故障，也常常需要人工去诊断等。

4.4.3 设计方案

本设计主要用于楼宇水表的自动抄表，抄表人员可以不用进入各个住户而将表数据读回。总体设计为首先在单元楼内安装一个ZigBee数据采集模块，用于方便读表人员收集各住户水表数据；同时还要在各住户家中安装一ZigBee远程用户终端模块，其主要用来读取水表的数据然后通过ZigBee的射频部分将数据传输到ZigBee的数据采集模块，如图4-12及图4-13所示。

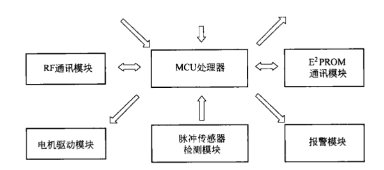


图4-12 模块内部结构

本设计采用 MESH 网状网络结构，保证数据传输的可靠性，每户每表设置一个 ZigBee 节点，每幢单元楼设置一个 ZigBee 路由节点，一个小区设置一个 ZigBee 中心节点，ZigBee 中心节点数据通过 GPRS 或网络上传到集抄中心。

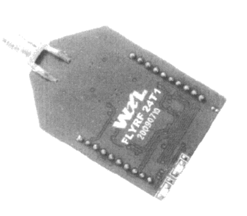


图4-13 模块外观

在 ZigBee 远程用户终端模块和 ZigBee 数据采集模块中，ZigBee 部分采用的是国内某公司近期推出的最新 2.4G 的 ZigBee 无线模块，ZigBee 无线模块只需要很少的外围器件且该器件无需了解繁琐的全功能 ZigBee 协议栈，从而减少开发时间并简化了 ZigBee 功能。ZigBee 无线模块不仅能够通过 SPI 或 UART 接口与各种 MCU 通信，还能与 TI 的 MPS430 超低功耗 MCU 等器件相结合。Z-stack 软件 ZigBee2006 协议栈可以在 ZigBee 处理器上运行，而应用程序则能在外部 MCU 上运行。ZigBee 无线模块能够处理所有时序关键型与处理密集型 ZigBee 协议任务，而将应用 MCU 的资源占用的空间释放出来用于满足其他程序的要求。

ZigBee 远程用户终端模块安装于单元楼中各住户家中。ZigBee 远程用户终端模块中，数据线 1、2、3 用于通过三线译码来控制水表某位的数据；数据线 4、5、6、7 用于显示水表某位上的数据；8 为地线。例如，数据线 1、2、3 状态为 000，则 4、5、6、7 位显示数字为水表第一位数字读数；数据线 1、2、3 状态为 111，则 4，5，6，7 位显示数字为水表第八位数字读数。在每一位读数后分别送入 ZigBee 模块进行处理。

ZigBee 数据采集模块安装于单元楼中的一层或比较方便读表员读表的位置。当 ZigBee 模块收到数据时通过 LED 驱动芯片将数据输出到 LED 显示器上，这样读表人员就可以清楚读数，其中前两位用于显示各住户的房间号，后六位用于显示对应房间号的水表数据。键盘用于控制 LED 显示器。

以 ZigBee 网络技术为支撑的无线自动抄水表系统，相比人工抄表方式或其他自动抄水表系统大大降低了运行成本和功耗，工作效率明显提高，节点硬件也易于实现，避免了有线抄表系统施工布线带来的各种问题。本设计提出的方案，硬件已经实现，当用户用水时

用户水表的液轮滚动，ZigBee 远程终端用户模块通过译码方式采集到水表数据，然后通过此模块的射频部分传输到 ZigBee 数据采集模块。

本系统需要长期在线连续运行，故对其可靠性和长期稳定性有较高的要求，在设计时给予重点考虑。本系统采用集成芯片作为电路的核心部分，大大减少了外扩电路的接线和使用的元器件的数目，使整机趋于微型化，也提高了整机的可靠性。

设计电路板时注意线的走向以及整机的紧凑性，在电路和工艺设计上采用各种成熟的实用抗干扰措施，例如合理布局、正确选择接地点、弱信号传输线屏蔽层单端接地、单元电路的封闭式屏蔽环等，以降低干扰水平。

重要数据进行多次备份，实时刷新处理，使用存储容量大的 EEPROM 来备份 RAM 数据。避免由于干扰造成的数据出错，EEPROM 的数据可以保持 10 年以上，数据保持不需后备电源。软件写入 EEPROM 采取必要的校验方式，保证数据的安全性。

系统需要具有极强的抗电磁干扰能力，以使数据的安全性得到进一步的提高。

由于本系统用电池供电，对功耗要求较高，在整个系统的软硬件设计时应引起足够的重视，例如元器件的选型，元器件的供电方式是用 I/O 供电还是直接用电源供电，单片机的选型等都是功耗能否降低的重要因素，当然软件设计也是决定功耗能否降低的重要因素，此部分在软件设计部分论述。

4.4.4 关键源码

ZigBee 协调器将扫描 DEFAULT_CHANLIST 指定的通道，最后在其中之一上形成网络。如果 ZDAPP_CONFIG_PAN_ID 被定义为 0xFFFF，那么协调器将根据自身的 IEEE 地址建立一个随机的 PAN ID，如果 ZDAPP_CONFIG_PAN_ID 没有被定义为 0xFFFF，那么协调器建立网络的 PAN ID 将由 ZDAPP_CONFIG_PAN_ID 指定。

当所有的参数配置好后，可以调用下面函数来格式化网络：

```
NLME_NetworkFormationRequest(
                                zgConfigPANID,
                                zgDefaultChannelList,
                                zgDefaultStartingScanDuration,
                                beaconOrder,
                                superframeOrder,
                                false
                                );
```

一般用 ZDO_StartDevice( ) 函数来启动一个设备。初始化函数应该初始化该任务的所有初始量，如相关硬件初始化，表格初始化，电源初始化等。下面代码中有详细的注释，程序清单如下所示：

```
//*******************************************************************
//函数原型:void SAPI_Init( byte task_id)
//输入：任务 ID
//输出：无
//功能描述：初始化任务
```

```
//************************************************************************
void SAPI_Init(byte task_id)
{
  uint8 startOptions;
  sapi_TaskID = task_id;  //分配任务 ID
  sapi_bindInProgress = 0xffff;  //不允许绑定过程
  sapi_epDesc.endPoint = zb_SimpleDesc.EndPoint;  //初始化描述符
  sapi_epDesc.task_id = &sapi_TaskID;  //
  sapi_epDesc.simpleDesc = (SimpleDescriptionFormat_t *)&zb_SimpleDesc;
  sapi_epDesc.latencyReq = noLatencyReqs;
  //在 AF 层登记该端点描述符
  afRegister(&sapi_epDesc);
  //关闭匹配描述符响应
  afSetMatch(sapi_epDesc.simpleDesc->EndPoint,FALSE);
  //从 ZDApp 登记返回事件
  ZDApp_RegisterForNwkAddrRsp(sapi_TaskID);
  ZDApp_RegisterForMatchDescRsp(sapi_TaskID);
#if(HAL_KEY == TRUE)
  //登记 HAL（键盘）事件
  RegisterForKeys(sapi_TaskID);
#endif
#if(defined HAL_KEY)&&(HAL_KEY == TRUE)
  if(HalKeyRead() == HAL_KEY_SW_1)
   {
    //关闭自动启动设备，复位
    startOptions = 0;
    zb_WriteConfiguration(ZCD_NV_STARTUP_OPTION,sizeof(uint8),&startOptions);
    zb_SystemReset();
   }
#endif
  //设置事件，启动应用
  osal_set_event(task_id,ZB_ENTRY_EVENT);
  }
```

任务事件处理函数，程序清单如下一段程序所示。处理该任务所有的事件，包括时间、消息和其他用户定义的事件。里面的所有确认函数，都是用户编写，向应用（用户）指示该事件发生，继而可以做相关的处理，如发现网络设备后，可以把该设备的信息输出到 LCD 或串口；接收到数据后，把该数据输出到 LCD 或串口。接收到命令后，根据命令做相应的处理（闪灯等）。发生键盘事件，可以调用键盘处理函数。发送完数据包后可以闪烁 LED 指示发送完毕等。

虽然能做很多处理，但是在本实验中很多事件虽然调用了函数，但是该函数没有做任何的处理，就有待于用户自己开发，如发送数据确认函数 zb_SendDataConfirm 就为空。当

然用户也可以添加自己的消息，在该实验中，为用户留下了空间 pMsg- > event > = ZB_USER_MSG。

```
//*****************************************************************
//函数原型:UINT16 SAPI_ProcessEvent(byte task_id,UINT16 events)
//输入: 任务 ID, 事件
//输出: 无
//功能描述: 初始化任务
//*****************************************************************
UINT16 SAPI_ProcessEvent(byte task_id,UINT16 events)
{
  osal_event_hdr_t * pMsg;
  afIncomingMSGPacket_t * pMSGpkt;
  afDataConfirm_t * pDataConfirm;
  ZDO_NwkAddrResp_t * pNwkAddrRsp;
  ZDO_MatchDescResp_t * pMatchRsp;
  zAddrType_t srcAddr,dstAddr;
    if(events & SYS_EVENT_MSG)        //同步消息事件
    {
    pMsg = (osal_event_hdr_t * )osal_msg_receive(task_id);
    while (pMsg)
     {
      switch(pMsg- > event)
       {
        case AF_DATA_CONFIRM_CMD:          //AF 数据确认
          //数据包发送确认信息.
          //这些状态值定义在 ZComDef. h 文件中 h
          //该信息定义域在 in AF. h 中
          pDataConfirm = (afDataConfirm_t * )pMsg;
          SAPI_SendDataConfirm(pDataConfirm- > transID,pDataConfirm- > hdr. status); //发送数据确认
          break;
        case AF_INCOMING_MSG_CMD:   //AF 数据输入
          pMSGpkt = (afIncomingMSGPacket_t * )pMsg;
          //接收数据指示
          SAPI_ReceiveDataIndication (pMSGpkt- > srcAddr. addr. shortAddr, pMSGpkt- > clusterId,
                                      pMSGpkt- > cmd. DataLength, pMSGpkt- > cmd. Data);
          break;
        case ZDO_STATE_CHANGE:            //ZDO 状态改变
         //向应用通报设备启动,
          if (pMsg- > status == DEV_END_DEVICE ||
              pMsg- > status == DEV_ROUTER ||
              pMsg- > status == DEV_ZB_COORD)
           {
```

```
        SAPI_StartConfirm(ZB_SUCCESS);          //启动确认
      }
      break;
    case ZDO_NWK_ADDR_RESP:   //网络地址响应
      //发现到设备，返回设备信息到应用
      pNwkAddrRsp = (ZDO_NwkAddrResp_t * )pMsg;
      SAPI_FindDeviceConfirm(ZB_IEEE_SEARCH,(uint8 * )&pNwkAddrRsp- > nwkAddr,
                                              pNwkAddrRsp- > extAddr);
      break;
    case ZDO_MATCH_DESC_RESP:   //ZDO 接收到一个匹配描述符响应
      pMatchRsp = (ZDO_MatchDescResp_t * )pMsg;
      if(sapi_bindInProgress ! = 0xffff)
       {
        //创建一个绑定表格条目
        srcAddr.addrMode = Addr16Bit;
        srcAddr.addr.shortAddr = _NIB.nwkDevAddress;
        dstAddr.addrMode = Addr16Bit;
        dstAddr.addr.shortAddr = pMatchRsp- > nwkAddr;
        if(APSME_BindRequest(&srcAddr,sapi_epDesc.simpleDesc- > EndPoint,
                sapi_bindInProgress,&dstAddr,pMatchRsp- > epList[0]) == ZSuccess)
         {
          osal_stop_timer(ZB_BIND_TIMER);
          osal_start_timerEx(ZDAppTaskID,ZDO_NWK_UPDATE_NV,250);
          sapi_bindInProgress = 0xffff;
          //发现 IEEE 地址
          ZDP_IEEEAddrReq(pMatchRsp- > nwkAddr,ZDP_ADDR_REQTYPE_SINGLE,0,0);
          //发送绑定确认，反馈到应用
          zb_BindConfirm(sapi_bindInProgress,ZB_SUCCESS);
         }
      }
      break;
    case ZDO_MATCH_DESC_RSP_SENT:            //ZDO 发送一个匹配描述符响应
      SAPI_AllowBindConfirm(((ZDO_MatchDescRspSent_t * )pMsg)- > nwkAddr);
      break;
    case KEY_CHANGE:  //键盘事件
      zb_HandleKeys(((keyChange_t * )pMsg)- > state,((keyChange_t * )pMsg)- > keys);
      break;
    case SAPICB_DATA_CNF:   //发送数据确认
      SAPI_SendDataConfirm((uint8)((sapi_CbackEvent_t * )pMsg)- > data,
                         ((sapi_CbackEvent_t * )pMsg)- > hdr.status);
      break;
case SAPICB_BIND_CNF:           //绑定确认
  SAPI_BindConfirm(((sapi_CbackEvent_t * )pMsg)- > data,
```

```
                    ((sapi_CbackEvent_t * )pMsg) - > hdr. status);
      break;
    case SAPICB_START_CNF:   //  设备启动确认
      SAPI_StartConfirm(((sapi_CbackEvent_t * )pMsg) - > hdr. status);
      break;
    default:
      //用户信息处理
      if(pMsg- > event > = ZB_USER_MSG)
       { //用户可以编写自己的消息处理任务函数  }
      break;
    }
  //释放存储空间
  osal_msg_deallocate((uint8 * )pMsg);
  //下一个任务事件
  pMsg = (osal_event_hdr_t * )osal_msg_receive(task_id);
  }
  //返回没有被处理的事件
  return(events ^ SYS_EVENT_MSG);
}
if(events & ZB_ALLOW_BIND_TIMER)  //允许绑定时间事件
{
  afSetMatch(sapi_epDesc. simpleDesc- > EndPoint,FALSE);
  return(events ^ ZB_ALLOW_BIND_TIMER);
}
  if(events & ZB_BIND_TIMER)  //绑定时间事件
{
  //Send bind confirm callback to application
  SAPI_BindConfirm(sapi_bindInProgress,ZB_TIMEOUT);
  sapi_bindInProgress = 0xffff;
  return(events ^ ZB_BIND_TIMER);
}
if(events & ZB_ENTRY_EVENT)  //设备启动事件
{
  uint8 startOptions;
  //等待启动事件
  HalLedSet(HAL_LED_4,HAL_LED_MODE_OFF);
  zb_ReadConfiguration(ZCD_NV_STARTUP_OPTION,sizeof(uint8), &startOptions);
    if(startOptions & ZCD_STARTOPT_AUTO_START)
      {
      zb_StartRequest();
    }
    else
      {
```

```
      //闪烁 LED2，等待外部输入，启动设备
      HalLedBlink(HAL_LED_2,0,50,500);
    }
    return(events^ZB_ENTRY_EVENT);
  }
  //用户事件必须是最后一个
  if(events &(ZB_USER_EVENTS))
  {
    //用户事件处理，这里函数没有编写
    zb_HandleOsalEvent(events);
  }
  //Discard unknown events
  return 0;
}
```

串口发送函数很简单，本实验中的串口发送函数为一个自定义的函数，这个函数的功能实现了发送一个字符串的功能，代码一共 3 句话，很简单，可以通过代码中的注释理解，程序清单如下所示：

```
/*******************************************************************
* 函数功能:串口发送字符串函数
* 入口参数:data:数据
*           len:数据长度
*******************************************************************/
void UartTX_Send_String(char * Data,int len)
{
  int j;
  for (j=0; j<len; j++)
  {
    while (!(IFG2&UCA0TXIFG));        //清除中断标志
    UCA0TXBUF   = * Data ++;          //发送数据
  }
}
```

串口接收中断函数主要实现两个功能，第一是读取串口接收到的数据，第二个功能是设置启动串口事件，将串口发生中的信息告诉操作系统，程序清单如下所示：

```
/*******************************************************************
* 函数功能:串口接收中断处理函数
* 入口参数:port:端口
*           event:事件
*******************************************************************/
static void rxCB(uint8 port,uint8 event)
{
  uart_Rx_count = HalUARTRead(0,rxBuf,uart_Rx_count);         //读串口的数据
```

```
    osal_set_event(SampleApp_TaskID,UART_RX_CB_EVT);          //设置串口事件
}
```

串口读取函数在这里直接采用了 Z-stack 中的函数库中提供的串口读取函数，这个函数的原型在 hal_uart. c 中，但是在使用中对其进行了局部的修改，修改如下。

修改前：

```
if(length > bufLength)
    length = bufLength;
```

修改后：

```
//if(length > bufLength)
    length = bufLength;
```

读取串口接收到的数据的函数程序清单如下所示：

```
/*******************************************************************
* 函数功能:串口接收函数
* 入口参数:port    :端口
           pBuffer:接收的数据
*          length:长度
* 返回值:接收到的数据长度
*******************************************************************/
uint16 HalUARTRead(uint8 port,uint8 * pBuffer,uint16 length)
{
  uint16 bufLength = Hal_UART_RxBufLen(0);        //读取串口数据长度
  uint16 x =0;
  /* 如果串口没有配置则读取 */
  if(uartRecord. configured)
  {
    //if(length > bufLength)
      length = bufLength;               //将接收到的数据长度赋值为 length
    if(pBuffer)                         //如果有数据
    {
      for(x =0;x < length;x ++)
      {
        pBuffer[x] = uartRecord. rx. pBuffer[uartRecord. rx. bufferHead ++];  //读取数据
        if((uartRecord. rx. bufferHead) == uartRecord. rx. maxBufSize)
          uartRecord. rx. bufferHead =0;
      }
      return length;                    //返回长度
    }
  }
  return 0;                             //返回 0
}
```

本实验中设计了广播和单播两种发送方式，两种发送方式在上节中已经给介绍了定义方法，在这里就不再介绍。值得注意的是，在本实验中设计的两个发送函数都拥有自己的传递参数，程序清单如下所示：

```
/***********************************************************************
 * 函数名:SampleApp_Send_All_Message
 * 功能描述: 数据广播发送
 * 参数: buff: 发送的数据
        Length: 数据长度
 * 返回: NULL
***********************************************************************/
void SampleApp_Send_All_Message(uint8 * buff,int length)
{
  if( AF_DataRequest( &SampleApp_All_DstAddr,&SampleApp_epDesc,
                      SAMPLEAPP_FLASH_CLUSTERID,
                      length,
                      buff,
                      &SampleApp_TransID,
                      AF_DISCV_ROUTE,
                      AF_DEFAULT_RADIUS) == afStatus_SUCCESS)
    {
    }
    else
    {
    }
  }
/***********************************************************************
 * 函数名:SampleApp_Send_All_Message
 * 功能描述: 数据广播发送
 * 参数: buff: 发送的数据
        Addr: 接收设备的短地址
        Length: 数据长度
 * 返回: NULL
***********************************************************************/
  void SampleApp_Send_Message( uint8 * buff,uint16 Addr,int length)
   {
      SampleApp_Single_DstAddr. addr. shortAddr = Addr;
      if( AF_DataRequest ( &SampleApp_Single_DstAddr,&SampleApp_epDesc,
                      SAMPLEAPP_FLASH_CLUSTERID,
                      length,
                      buff,
                      &SampleApp_TransID,
                      AF_DISCV_ROUTE,
```

```
                    AF_DEFAULT_RADIUS) == afStatus_SUCCESS)
      {
      }
    else
      {
      }
  }
```

ZigBee 接收处理函数的作用在本实验中很重要，设备在接收到数据后，就会通过事件调用该函数，程序清单如下一段程序所示。下面来分解这个函数的功能。

首先，无论接收到什么数据，小灯均会闪烁四次，表示通信正常收到了数据；然后将数据拷贝到一个数组中，方便处理；接下来就是处理这些数据，如果判断是查看节点命令的话，则首先读取本机的网络地址，然后将本机的网路地址转换为可见字符，发送给发送命令的设备。

如果不是命令，则直接将接收到的数据发送给串口，接收处理的流程就完成了。

```
/*****************************************************************
* 函数名:SampleApp_MessageMSGCB
* 功能描述：数据回收处理
* 参数：afIncomingMSGPacket_t
* 返回：NULL
*****************************************************************/
void SampleApp_MessageMSGCB(afIncomingMSGPacket_t * pkt)
{
  uint8 Rx_Buf[50];
  uint8 temp;
  switch(pkt->clusterId)
  {
    case SAMPLEAPP_PERIODIC_CLUSTERID:
      break;
    case SAMPLEAPP_FLASH_CLUSTERID:
      HalLedBlink(HAL_LED_4,4,50,(1000/4));                //小灯闪烁
      memcpy(Rx_Buf,pkt->cmd.Data,pkt->cmd.DataLength);     //将数据拷贝到数组
      if(! strncmp((char *)Rx_Buf,(char *)Find_Cmd,9))      //判断命令
      {
        RfTx.ADDRDATA.Saddr = NLME_GetShortAddr();          //读取本机网络地址
        temp = RfTx.addr_temp[0];                            //交换位置
        RfTx.addr_temp[0] = RfTx.addr_temp[1];
        RfTx.addr_temp[1] = temp;
        RfTx.TXDATA.addr[0] = RfTx.addr_temp[0]/16;         //数据位处理
        RfTx.TXDATA.addr[1] = RfTx.addr_temp[0] % 16;
        RfTx.TXDATA.addr[2] = RfTx.addr_temp[1]/16;
        RfTx.TXDATA.addr[3] = RfTx.addr_temp[1] % 16;
```

```
for(int i=0;i<4;i++)                                          //转换位可见字符
{
  if((RfTx.TXDATA.addr[i]>=0)&&(RfTx.TXDATA.addr[i]<=9))
  {
    RfTx.TXDATA.addr[i]+=48;
  }
  else
  {
    switch(RfTx.TXDATA.addr[i])
    {
    case 10:
      RfTx.TXDATA.addr[i]='A';
      break;
    case 11:
      RfTx.TXDATA.addr[i]='B';
      break;
    case 12:
      RfTx.TXDATA.addr[i]='C';
      break;
    case 13:
      RfTx.TXDATA.addr[i]='D';
      break;
    case 14:
      RfTx.TXDATA.addr[i]='E';
      break;
    case 15:
      RfTx.TXDATA.addr[i]='F';
      break;
    }
  }
}
RfTx.TXDATA.hex[0]='0';                                  //补充为16进制表示方法
RfTx.TXDATA.hex[1]='x';
//发送短地址
SampleApp_Send_Message(RfTx.short_address,pkt->srcAddr.addr.shortAddr,6);
}
else                                                       //不是命令则发送到串口
UartTX_Send_String((char *)Rx_Buf,pkt->cmd.DataLength);
UartTX_Send_String("\n",sizeof("\n"));                     //换行方便查看
break;
}
}
```

4.5 智能能源管理应用设计实例

网络时代的发展，应引入智能化的概念。在传统的楼宇自控系统中，一般只包括了综合布线、计算机网络、安防、消防、闭路电视监控等子系统。但近年来，随着经济的发展和科技的进步，人们对照明灯具节能和科学管理提出了更高的要求，使得照明控制在智能化领域的地位越来越重要。而在楼宇大厦建设热潮中，各大公司企业和它们的建设者也意识到了智能照明的重要性。商业楼宇大功率动力和制冷设备比重较少，照明灯具则相对比重更多。使用照明控制系统，更能体现其在节能与管理方面的优势，提高学校的科学管理水平。

节能是照明控制系统的最大优势。传统的楼宇公共区域照明工作模式，只能是白天关灯，晚上开灯。而采用了智能照明控制系统后，我们可以根据不同场合、不同的人流量，进行时间段、工作模式的细分，把不必要的照明关掉，在需要时自动开启。同时，系统还能充分利用自然光，自动调节室内照度。控制系统实现了不同工作场合的多种照明工作模式，在保证必要照明的同时，有效减少了灯具的工作时间，节省了不必要的能源开支，也延长了灯具的寿命。

良好的工作环境是提高工作效率的一个必要条件。合理地选用光源、灯具及性能优越的照明控制系统，都能提高照明质量。智能照明控制系统具有开关和调光两种控制方法，可以有效地控制各种照明场所的平均照度值，从而提高照度均匀性。同时系统能根据不同的时间段，人们的不同需要，自动调节照度。

智能照明控制系统是以自动控制为主、人工控制为辅的系统。在一般的情况下，不需要有人的参与，照明系统自动实现开关和调光功能。既大大减少了管理人员的数量，也排除了由于人为因素而出现的不定时开关，影响学校的正常教学、生活秩序的情况出现。

智能照明控制系统在节能和节省灯具使用的同时，有效节省了电费与管理费用的支出。根据一般的办公大楼运营的经验来看，节能效果能达到 40% 以上，一般的商场、酒店、地铁站等节能效果也能达到 25% ~30%；学校在这方面还没有得到具体的统计数据，但根据分析，效果还是令人满意的。

4.5.1 智慧能源

根据智能建筑专家的估计，如果在建筑物中大量采用感应、定位、智能控制和多能源优化等普通信息技术以及分布式能源、热电冷梯级利用和蓄能等成熟技术，实现了建筑的“精确供能”，就可以在人们需要的地方、需要的时间、需要能源的品种（电、热、冷）针对性地供应能源，以现有 1/2 能耗就可以维持比现在更加舒适的生活品质。如果进一步进行建筑结构的围护结构节能，并使用更新型的可再生能源、废能回收技术等，建筑能源消耗还会减少 1/2，也就是说未来 1/4 的能源足以让我们生活得更好、更舒适。

一个建筑或一座工厂最大的电耗来自电机系统，如电梯、水泵、风机、空调、洗衣机、电冰箱等，一般电动机启动负荷是正常运行的 5 ~7 倍，采用变频控制软启动技术也要 1.5 倍的电流强度。现在的建筑设计师通常将所有的电机负荷简单相加，再乘以一个巨大的安全系数，结果是变压器容量巨大，输电线路投资巨大，电力系统负荷损耗巨大。如果我们能对每一个电机进行优化控制，避免它们同时开启，就可以将变压器容量缩小到

1/3至1/5，变压器的损失随之减少。

"随手关灯"总有关不到的地方和时候，如果采用智能感应照明，只在有人有需求的地方进行精确照明，可以环顾一下我们的家庭或办公场所，估算一下可以节省多少电能，减排多少二氧化碳。而实现这一技术仅需要为每一个灯口安装一个芯片和控制开关，在适当的地方安装感应器，相关的控制数据信息可以直接从无线上传送。

IBM公司CEO彭明盛最近发表了关于《智慧的地球》演讲，他认为世界正在从互联网，进入到"物联网"（the Internet of things）的时代，全人类的智慧化将实现"无所不在的连接（pervasive connectivity）"。

北京有近2000万人口，约500万台冰箱，如果以每台冰箱120W，合计装机负荷60×10^4kW，如果未来的冰箱可以蓄冰储能，所有冰箱都在夜间用电低谷蓄冰，并根据电网的智能安排分批进行工作，电网就可以因此减少几十万千瓦的装机和相应输电线路和变电站的建设投资和运行损耗。电热水器、电动汽车也可采用同样模式，在低谷蓄电，并由智能电网进行负荷平衡安排。可见未来的智能电网将会使人类进行各种各样的创造，设计制造各种新的和超出我们目前想象力的新产品，改变我们的生活。

未来要减少温室气体排放，就必须大量使用可再生能源，而可再生能源存在不稳定的特性，风电是有风有电，无风无电；水电是丰水有电，枯水无电；太阳能更是有太阳有电，无太阳无电，哪怕是一朵云彩，也会引起供电的波动；甚至是天然气的热电冷系统，也可能因为燃气管网的用气波动而不能稳定发电、供热、制冷。智能电网要将这些电源管理起来，将各种能源系统融合在一起，使各种能源互相弥补，再配合蓄电技术及蓄热、蓄冷技术，同时对用电终端进行优化配置，使供需之间和各用户之间以及各种电源之间现遥相呼应，互补互助。也只有建立这样的系统，可再生能源才可能成为一种有价值的能源供应形式，这就必须为电网植入智慧。

对于这种能源系统，国际社会称之为"智慧能源（intelligent energy）"，与之相关的技术就是"智慧能源技术"。这是一个包含各种形式的能源资源，特别是低碳的天然气和可再生能源，各种形式的能源转换技术和各种各样的能源使用终端设施，在智能化信息系统的控制下联成一个整体，调动全社会多元的创造性，共同解决人类面临的问题。而最终需要实现的目标是将能源效率不断提高，有效控制全球气候变化的趋势，从经济、社会、环境和资源上实现真正意义的可持续发展，而这一技术革命将不可避免地影响人类未来的社会经济、政治。

4.5.2 智能能源实例——照明控制系统

随着社会的进步，节能和环保已是大势所趋，在照明领域中，采用新型节能光源、节能电器及高效灯具来达到节约电能的目的，已广泛被人们所接受。但如何通过节能照明设计来达到节约能源的目的才刚被人们重视。基于有线的照明控制系统，具有布线麻烦、增减设备需要重新布线、系统可扩展性差、系统安装和维护成本高以及移动性能差等缺点，因此无线通信技术是实现智能照明系统的理想选择。近年来，近距离无线通信技术获得了迅猛的发展。其中主流技术包括红外技术、蓝牙（Bluetooth）、Wi-Fi、UWB（Ultra-Wideband）和ZigBee技术等。它们都有各自的标准、特点和相应的应用领域，另外还有Z-Wave和MiWi等专有无线技术。智能照明系统自身的要求和ZigBee技术具有的特点，决

定了 ZigBee 是实现无线智能照明系统的最佳解决方案。

无线智能照明系统的控制器与照明灯节点之间只需传输开关信号和调光信号等开光量，且数据发送频率不高，而 ZigBee 的最大传输速率可以达到 250kb/s，这对于实现无线智能照明系统来说已经足够；无线智能照明系统的各个灯节点往往需要组成一个星型网、簇状网或者网状网，节点数量在几十到几千个之间，ZigBee 对以上拓扑结构都做了很好的支持，且网络最大节点数可达 65535，很好地满足了无线智能照明系统对网络结构及容量的要求，而这是蓝牙和红外技术所无法满足的；不同厂家生产的无线智能照明系统的各种节点之间要求具有互操作性，ZigBee 是一个开放式全球标准，世界各大 ZigBee 方案提供商都通过 ZigBee Alliance 的兼容性测试，并且 ZigBee Allianee 针对照明系统，专门制定了相应的 Profile，因此不同厂家基于 ZigBee 技术开发的灯节点之间可以进行互操作和相互替换，从而保障生产商和用户的利益和成本投入，这是 Z-Wave 和 MiWi 等专有的无线技术所无法满足的。

智能照明系统，比如智能家居，需要所有房间和楼层间的通信，这就需要系统具有穿墙的信号传递功能和网络功能，ZigBee 工作在 2.4GHz 的 ISM 频段，节点之间的最大通信距离可达 100m，信号具有一定的穿墙能力，并且 ZigBee 支持路由节点，只要合理布局，可以保证建筑物内没有无线通信的盲区，这是红外技术所无法提供的；ZigBee 具备较快的响应特性，2 个节点之间的一次数据发送过程在 5ms 之内即可完成，满足照明系统对实时性的要求；照明系统对成本非常敏感，这将决定它能否实用化和产业化，ZigBee 是一种低速率、低成本的无线通信技术，相比于 Wi-Fi 和 UWB 等这些适用于无线局域网和多媒体应用的高速率无线标准而言，成本非常低廉。

4.5.3　智能照明设计目标

采用智能照明控制系统后，可使照明系统全自动运行，系统将按照预先设置切换到若干不同的基本工作状态，如“白天”、“晚上”、“周末”、“清洁”等，根据预设的时间自动地在各种工作状态之间进行转换。此外，对于高档办公楼的大厅、会议室等场所，则可以根据一天的不同时间、不同用途精心地进行灯光的场景预设置，使用时只需调用预先设置好的最佳灯光场景，就可使人们产生很好的视觉效果。

在大楼办公室，配备可调光电子镇流器的日光灯在智能照明控制系统下与传统的日光灯照明系统相比具有显著的优势：因为配有传统镇流器的日光灯会以 100Hz 频率闪动，这种频闪使工作人员头晕，眼睛疲劳，降低了工作效率。而可调光电子镇流器在工作时需要很高频率（40 ~ 70kHz），不仅克服了频闪，而且消除了由于使用启辉器而造成启动灯时亮度的不稳定，改善了办公环境，提高了工作效率，这一点也给管理者带来了巨大的经济回报。

一般照明设计在对新的办公用房进行照明设计时，由于考虑到照度衰减，设计的照度通常比要求的要高。而这样设计的结果就是新房间照度偏高，使办公用房使用期照度不一致，而且照度偏高也会造成不必要的能源浪费。在智能照明控制系统下，由于可以进行智能调光，尽管照度还是偏高设计，但系统将会按照预先设置的标准亮度使办公室在使用期内保持恒定照度，而不受灯具效率降低和墙面反射系数衰减的影响。

现代办公建筑的节能和降低运行费用是受人们关注的重要课题。按照国际标准，办公

室的最佳光照度应为400lx，智能照明控制系统能利用智能优感器感应室外光线，自动调节光照度，以达到节能效果，同时也可采用时钟管理器对照明进行定时控制。

灯具遭受损坏的致命原因是电网过电压，灯具的工作电压越高，其寿命就越低，所以适当降低灯具工作电压是延长灯具寿命的有效途径。

智能照明控制系统能成功地抑制电网的冲击电压和浪涌电压，使灯具不会因为上述原因而过早损坏。同时，还可以通过系统人为地确定电压限制，提高灯具寿命，这样不仅节省了大量灯具，而且大大减少了更换灯具的工作时间，有效地降低了照明系统的运行费用。

4.5.4 智能照明控制系统组成

智能照明控制系统具有和传统跷板开关一样的控制功能、调光功能，而且有自动探测设备能感测如人体运动和周围环境照度等，自动控制灯的开关及调光，还可以与其他的自控系统集成，实现相互控制。智能照明控制系统分为硬件和软件两大部分，其中硬件主要由输入单元、输出单元、系统单元三部分组成，软件则由编程软件、监控软件、时控软件组成，硬件通过总线系统连接成网络，由软件实现远程自动控制。

输入单元将外界控制信号转变为系统信号在总线上传播，一般输入单元包括线式开关、场景控制器、遥控设备、红外及亮度优感器等。

输出单元接收总线上信号，控制相应回路输出，实现对负载进行控制。一般由继电器、调光器、模拟单元等组成。

系统单元由电源供应单元、PC 接口等组成。系统单元通过对各个输入、输出单元及计算机调制解调器的连接实现网络化连接，为集中及远程控制创造了条件。

编程软件通过与网络中 PC 接口相连的计算机随时修改系统的控制要求，是智能照明控制系统的大脑。

监控软件通过可视化界面，预先制定控制方案或临时对大楼内灯具进行开关、调光等控制，是控制系统的执行者。

时空软件可实现灯光按规律点亮或熄灭。

我们在进行设计之初应该将建筑按功能的不同进行分区，不同的区域对照明及控制的要求是不一样的。一般的办公建筑基本可以分为办公区、功能区、辅助区及室外照明等功能区域。

现代办公楼内普通办公区均以敞开式大空间为主，办公面积大，可以将整个办公区分成若干个独立的照明区域，采用网络开关根据需要开启相应区域的照明，由于出入口多，可实现办公区内多点控制，方便了使用人员操作。在每个出入口都可以开启和关闭整个办公区的所有灯，这样可根据需要方便就近地控制办公区的灯，同时可以根据时间进行控制，如平时晚 8 点自动关灯，如果有人加班，则可以切换为手动开关灯。

高级办公区一般都会进行个性化装修，而且灯具多，组合形式多样，可以通过多种控制方式对照明进行控制，这其中包括场景控制、遥控、调光控制等。可以在不同的环境，要求开启不同的灯具组合并进行调光等操作，如办公、会客、休闲，而这些都可以通过编程进行预设置，使用时只通过单键操作即可。

作为功能区的会议室、多功能厅等场所是办公楼的一个重要组成部分，通过场景设置

可以将其设定为会议报告状态、多媒体会议状态、娱乐休息状态、清扫状态等，真正使多功能场所在照明上实现多功能化。

作为辅助区的大厅、走廊、楼梯间、洗手间等场所，因为使用比较频繁、时间性强，一般以时间控制为主并结合安装红外感应器等方式以达到节约能源的目的。

大厅是进入办公楼的必经之路，使用时间段相对集中，如上下班时间，可以开启全部回路的灯光，方便人员进出，营造明亮洁净的气氛；人员进出较少时段可只打开部分回路灯光。此区域控制集中在管理室，可由就地控制、计算机控制、时间定时控制进行操作。

走廊作为各办公室空间的联络通道，照明也至关重要，我们主要采用自动控制方法。正常工作时间全开，非工作时间改为减光照明，如可只用1/3，节假日无人时可以只亮少许灯，同时在各出入口装设手动控制开关，可根据需要手动控制。

楼梯间在现代办公建筑中，尤其是高层建筑中已不作为主要通道而只作为辅助通道及应急疏散通道使用，所以控制方式以红外感应延时开关为主。人来开灯，人离开后延时关闭，这样可以大大地节约能源，而在火灾报警确认后，应急点亮楼梯间照明作为疏散照明，有利于人员疏散。

现代建筑中洗手间已显得越来越重要，是体现办公环境的重要环节。但这种地方也存在管理的盲区，普通管理方式下这里的灯经常成为长明灯，比较浪费。而智能化设计中采用红外感应进行控制，人来开灯，人走延时关闭或采用传统方式与时间控制相结合的方式，在平时由传统方式控制，晚间无人后通过定时将回路断开以节约能源。

由于现代大多数办公建筑均将停车场设在地下层内，地下室无自然采光，这就要求车场内有一部分照明需要常明，而办公建筑停车场忙闲时间又非常的明显和集中，这样我们就可以采用时间定时控制方式，可分为忙时照明、闲时照明、维持照明，忙闲分明，大大节约了能源。

泛光照明是建筑的一个闪光点，是凸显建筑特点的重要手段，但同时也是耗电的大户，如何扮靓建筑又减少不必要的浪费就显得尤为重要。我们在智能化系统中可主要通过日期设置及时间设置完成这个任务。在主控计算机上，对开启/关闭时间进行设定，如晚上 6 点开启整个泛光照明灯，10 点关闭部分灯，12 点以后只保留很少的灯或全部关闭，当然，还要根据一年四季昼夜长短的变化和节假日进行相应的调整。

智能照明控制系统可以很容易地通过开放通信协议利用网络连接到楼宇管理系统中而成为其子系统，尤其要强调的是智能照明控制系统管理着所有照明，其中也包括火灾应急照明。智能照明控制系统硬件设备上均设计有消防联动接口，火灾时可强行点亮应急照明以达到消防要求。

今后，智能照明控制系统必将朝着智能化、小型化、标准化的方向发展。网络系统更加优化，功能更加完善，扩展更加便捷，保护更加可靠，节能更加可观，其大面积的应用也将成为必然。

4.5.5 智能照明系统的实现

ZigBee 是一种在无线个人网络领域中新兴的无线网络技术。电子与电气工程师协会 IEEE 于 2000 年年底成立了 802.15.4 工作组，规定了 ZigBee 的物理层和媒体接入控制层。2001 年 8 月成立了 ZigBee 联盟，负责 ZigBee 规范的制定和应用推广工作，2004 年 12 月推

出 ZigBee 规范的正式版本 ZigBee SpecificationV1.0。目前，ZigBee 标准在 ZigBee 联盟的推动下正日趋增强和完善，其实际工程应用正日益普及。世界各大半导体巨头 TI、FreeScale 和 Ember 等各自推出了符合 ZigBee 标准的芯片及协议栈。其中 TI 公司的 CC2430 加 Z-Stack 协议栈是业内公认的最佳解决方案。

无线智能照明系统的网络节点分为协调器、路由器和终端节点三种。

协调器节点带有键盘，用来设置整个系统的参数和发送控制命令，128 ×64 汉字图形点阵液晶模块用于显示网络状态信息。微控制器输出开关量直接完成对照明灯的开关控制，微控制器输出数字量经过 8 位数/模转换器后，可以实现对照明灯的 256 级调光控制。

另外协调器节点还带有震动感测器和亮度感测器，用于感测现场的震动信息和亮度信息。当震动感测器测得震动较弱，即认为现场人员已经离开，此时可以自动关掉照明灯或者调暗亮度。当亮度感测器测得光线太亮，如晴朗的白天，即可自动调低亮度，当亮度感测器测得光线太暗，如夜晚或者阴雨的白天，即可调高亮度。系统只需在一个节点上集成震动感测器和亮度感测器，即可通过 ZigBee 网络向各个灯节点传输控制信息，实现对整个照明系统的智能控制，成本低廉。当然也可以将震动感测器和亮度感测器做成一个单独的 ZigBee 网络节点，用于感测现场不同位置的震动信息和亮度信息。

软件设计基于 TI 公司推出的与 CC2430 芯片配套的 Z-Stack 协议栈和 IAR 集成开发环境。针对 ZigBee 在家庭网络方面的应用，ZigBee Alliance 制定专门的应用框架，即 ZigBee Home Automation Public Application Profile。所谓 Profile 是对逻辑设备及其接口的描述集合，是针对某个特定应用的公约和准则，其目的是使不同厂家按照同一个 Profile 设计的产品之间可以相互操作、相互替换。ZigBee Home Automation Public Application Profile 规定了智能家居中的照明设备、采暖通风空调设备、自动窗帘和报警装置的设计规范。本节的无线智能照明系统就是在这个 Profile 的基础上实现的。Z-Stack 提供了丰富的函数调用接口。

在每盏灯中都集成有 ZigBee 模块，其中协调器节点是必需的。在其他地方，根据是否需要路由功能，可以配置为路由器或者终端节点。因为协调器节点和路由器节点具有路由功能，协议栈容量较大，所需的 FLASH 空间较大，芯片的成本也较高，因此只把需要给其他节点路由转发数据包的节点配置为路由器节点，其他节点则都配置为终端节点，以降低成本。室内所有的照明灯组成一个 ZigBee 网络，由协调器完成对所有照明灯的控制。可以对网络中的照明灯单个分别进行控制，也可以把所有的照明灯作为一个整体，进行同时控制；实现了对照明灯的简单开关控制和 256 级的调光控制；既可以设置成手动控制模式，也可以设置成自动控制模式，由协调器根据亮度感测器和震动感测器返回的亮度信息和震动信息，自动发送控制命令，完成对所有照明灯的控制。系统设计成本低廉，可靠性高、响应速度快、智能化程度高，是不断发展的电子信息技术在照明领域中的应用，必将带来照明技术的革新。

4.5.6 ZigBee 智能能源

随着计算机技术、通信技术、控制技术的发展和人们物质生活水平的提高，家居智能化正成为国内外的一个研究热点。基于 ZigBee 技术无线智能照明系统目前主要应用在智能大厦和高档住宅。但是随着技术水平的不断完善，相关产品的价格会逐步降低，巨大的民用市场将是最终的发展方向。该系统在提高照明系统的信息化、智能化程度的同时，对节

约电能的消耗也起到了很大的作用，符合国家节能减排的发展战略。

自2004年发布第一个规范以来，ZigBee标准现在已经发展成熟到能够获得全世界认可的地步，并开始在市场上发挥举足轻重的作用。ZigBee提供了一款高性价比、基于多种标准的无线网络解决方案，该解决方案支持以低数据速率、低功耗网络通信为重点的技术。到目前为止大多数ZigBee产品和部署仍然保持着一定的专属性，它们作为系统出售而非连接公共网络的某种设备。最近人们对于高级电表架构（AMI），或者更具体地说对智能能源管理的关注，是开放ZigBee标准使其成为真正可互操作的全球标准的契机，而这正是人们数年来所一直呼吁的。

“维基百科”对高级电表架构（AMI）的定义是“按照要求或事先定义的方案通过各种通信媒介从一些先进设备（例如电表、煤气计、水表等）对能源使用情况进行测量、收集和分析的系统。该架构包括硬件、软件、通信、与消费类电子相关的系统以及计量表数据管理软件”。

国家和地方政府要求一些电力公司制定支持动态定价的商业模型，以此来努力降低能源消耗和成本，并利用负载控制和需求响应来减少系统的峰值能源需求，在这种情况下AMI计划便应运而生了。其最初想法是向能源用户提供信息，鼓励他们节约能源，让他们对家中消耗能源的方式更加负责。很显然，该AMI计划远远不止是部署ZigBee标准那么简单，但是就本节而言，只重点阐述ZigBee在AMI计划中的作用。

为了支持AMI，ZigBee联盟定义并认可了智能能源管理文件。在一个由电表及自动调温器厂商、电力公司和其他相关各方组成的委员会内部对该文件细则进行了讨论，并最终确定了下来。“ZigBee智能能源管理”为电力企业提供了一种和众多“智能”设备及装置通信的安全机制，从而实现了家庭能源管理。

根据少数服从多数的原则，智能能源管理文件对电表、需求响应及负载控制、定价、文本通信及通知、安全和支持设备清单等进行了定义。更具体的讲，该文件定义了允许哪些设备可以添加到AMI网络（例如家庭用能源显示设备的网关、电表、水表、煤气表、自动恒温器、负载控制设备等）以及这些仪表之间必须支持的必要的或可选的通信。AMI的一个重要部分就是对实时定价的支持，这样便可以在一定的间隔时间内（例如15分钟）获得账单。

在需求高峰期间能源生产的成本大大增加（当电厂以接近最大效率运行时它就需要花费更多的资金来发更多的电）。因此，相对于今天统一费率的定价，建立和提供按时段定价既有利于电力企业也有利于消费者。时段定价意味着消费者的用电账单可以反映其实际用电费用。

对于那些想要省钱的人来说，关掉不用的电灯、拔下闲置电器的电源插头、外出时调低恒温计设置以及在电价便宜时段（及非用电高峰期）使用一些不那么重要的电器，例如洗碗机和洗衣机等，都可以受益于时段定价。这种用电方式的改变也会给电力企业带来好处。全体消费者的这种行为可以降低电的峰值消耗，并避免对于高成本（及低效益）发电的需求。

AMI和智能能源管理的运用既节省费用又有利于环保，而时段定价仅仅只是个开始。为了再进一步优化能源消费，智能能源管理还可支持事件计划安排以及对智能应用的外部控制，可基于计时定价重启（适用于HVAC系统）或者关闭（适用于水泵）这些应用。

就智能能源管理而言，其包括负载控制设备，可以由用户或者电力企业直接远程控制。智能能源管理还将其扩展至一个被称为 OpenHAN 的更大的范围。

OpenHAN 的主要功能是支持电力企业和家庭局域网（HAN）之间的双向通信。在一些建议方案中（对此还未最终定案），电力企业会对电表保持一种专有的通信基础结构，其将作为 ZigBee 智能能源管理网络的网关。该网络包括诸如上述一些设备，并支持一个负载与能源管理系统，而该负载与能源管理系统又包括智能能源管理网络中的负载控制器，以及连接单独存在的家庭自动化（HA）网络，如图 4-14 所示。

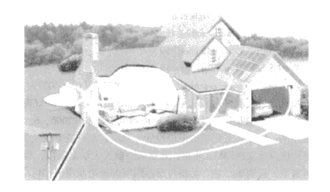


图 4-14 家庭智能能源示意图

整套系统提供对用电数据及定价的直接访问，并支持负载控制集成和可靠的按需降载双向通信。另外，它还保证能够利用未来产品及设备扩展 OpenHAN 的功能，这些产品和设备可以充分利用来自电力企业的数据。在这种情况下，智能能源管理网络基本由电力企业控制，而 HA 网络则保持对消费者开放。新型设备可以整合到该系统中，并基于服务提供商所提供的服务向电力企业注册。

虽然并非是首次试验性部署的一部分，也不是智能能源管理的核心，但是电力企业部署的这种架构将会成为未来智能能源管理技术的起点。我们可以想象在不远的将来，我们的洗衣机、干衣机、洗碗机、冰箱、水泵、灯具、空调、电视和其他电子设备以及无数其他家庭设备，都将连接到这个网络，可根据时间自动地开启和关闭，并在电价极高时关闭或者重启。在此情况下，一些设备将会由户主来控制，一些由电力企业控制，而其他的设备则可通过电力企业拥有控制权而户主也可手动控制的可选服务来控制，但是一些诸如医疗设备之类的重要设备将除外。

为了努力实现这一远景目标，2006 年 11 月的卡特威尔 AMR 报告（Chartwell AMR Report）预计未来四年内 AMI 技术将使自动电表的销量翻一番。美国有 1 亿个家庭，因此这一技术在美国会拥有广大的市场。通过部署 AMI 和智能电表，可以极大地节省能源和费用。

尽管最初主要是针对美国市场，但是智能能源管理也有望成为一个全球性标准，而其最先考虑的是成为欧洲和亚洲市场的解决方案。由于油价和电价几乎每天都创新高以及对煤资源枯竭及环境恶化的关注日益增长，我们可能会看到在不远的将来对于 AMI 和其他形式智能能源效益技术的需求将不断增加。ZigBee 就是这样一种可以带来无限可能的技术。

参 考 文 献

[1] CC2430 A True System-on-Chip solution for 2.4 GHz IEEE802.15.4/ZigBee. http://www.chipcon.com, www.TI.com.
[2] Bluetooth White Papers. http://www.bluetooth.com.
[3] STR91xV1.0 中文编程参考手册. http://www.mxchip.com.
[4] CC2431 System-on-Chip for 2.4 GHz ZigBee/IEEE802.15.4 with Location Engine. http://www.chipcon.com; www.TI.com.
[5] ZigBee Specification 2006. http://www.zigbee.org.
[6] ZigBee Specification 2004. http://www.zigbee.org.
[7] IEEE Std 802.15.4 2003. http://www.zigbee.org.
[8] 8051 IAR Embedded Workbench Help. http://www.iar.com/.
[9] 解析ZigBee堆栈架构. http://www.eetchina.com/ART_8800403003_640279_1fddbe6c.HTM.
[10] 如何建立完善的单片机开发实验平台. http://www.ourmpu.com/mcujx/kfdh00.htm.
[11] 陈丹，林金朝. 无线定位系统及其发展趋势[J]. 山西电子技术，2006，6.
[12] 贝克. 嵌入式系统译丛：嵌入式系统中的模拟设计. 北京：北京航空航天大学出版社，2005.
[13] 楼然苗. 51系列单片机设计实例[M]. 北京：北京航空航天大学出版社，2006.
[14] 王殊，阎毓杰，胡富平，屈晓旭，等. 无线传感器网络的理论及应用[M]. 北京：北京航空航天大学出版社，2005.
[15] Simon Haykin，Michael Moher. 现代无线通信[M]. 郑宝玉等译. 北京：电子工业出版社，2006.
[16] 周航慈. 单片机应用程序设计技术[M]. 北京：北京航空航天大学出版社，1991.
[17] 北京教育科学研究院. 无线电技术基础[M]. 北京：人民邮电出版社，2005.
[18] 郭兵. SOC技术原理应用[M]. 北京：清华大学出版社，2006.
[19] 赵阿群，陈少红，赵直，等. 计算机网络基础[M]. 北京：北京交通大学出版社，2005.
[20] 蒋挺，赵成. 紫蜂技术及其应用[M]. 北京：北京邮电大学出版社，2006.
[21] 徐爱钧，彭秀华. 单片机高级语言C51 Windows环境编程与应用[M]. 北京：电子工业出版社，2003.
[22] 李文仲，段朝玉. ZigBee无线网络入门与实战[M]. 北京：北京航空航天大学出版社，2007.
[23] 周立功，等，ARM嵌入式系统基础教程[M]. 北京：北京航空航天大学出版社，2005.